



Navigating Law To Share Data

The What, Who, Why and How

Denise Chrysler, J.D.
Colin Boes, J.D.

Data Summit October 3, 2019

The Fine Print



This presentation is for informational purposes only. It is not intended as a legal position or advice from us or our employers.

For legal advice, attendees should consult with their own counsel.

The Promise of Electronic Data

- » **Timely, reliable, granular data (i.e. sub-county) and actionable data**
- » **Many and diverse sources – including sources and types of data relevant to social and environmental determinants**
- » **Accessible to communities throughout the country that are shared, linked, and synthesized while protecting data security and individual privacy**
- » **Clear metrics to assess impact and document success**

A systematic review of barriers to data sharing in public health (2014)

1. **Technical**
2. **Motivational**
3. **Economic**
4. **Political**
5. **Legal**
 - a) Ownership and copyright
 - b) Protection of privacy
6. **Ethical**

Objectives

1. **Develop skills in defining and honing the use case**
2. **Provide systematic approach to identify and resolve legal, logistical, and security issues around data sharing**
3. **Improve understanding of data protection laws applicable to a use case, including opportunities these laws provide to share data as well as conditions, prerequisites and limitations they may impose**
4. **Understand security implications in various data sharing scenarios, including what red flags to look for in proposed use cases and best practices**

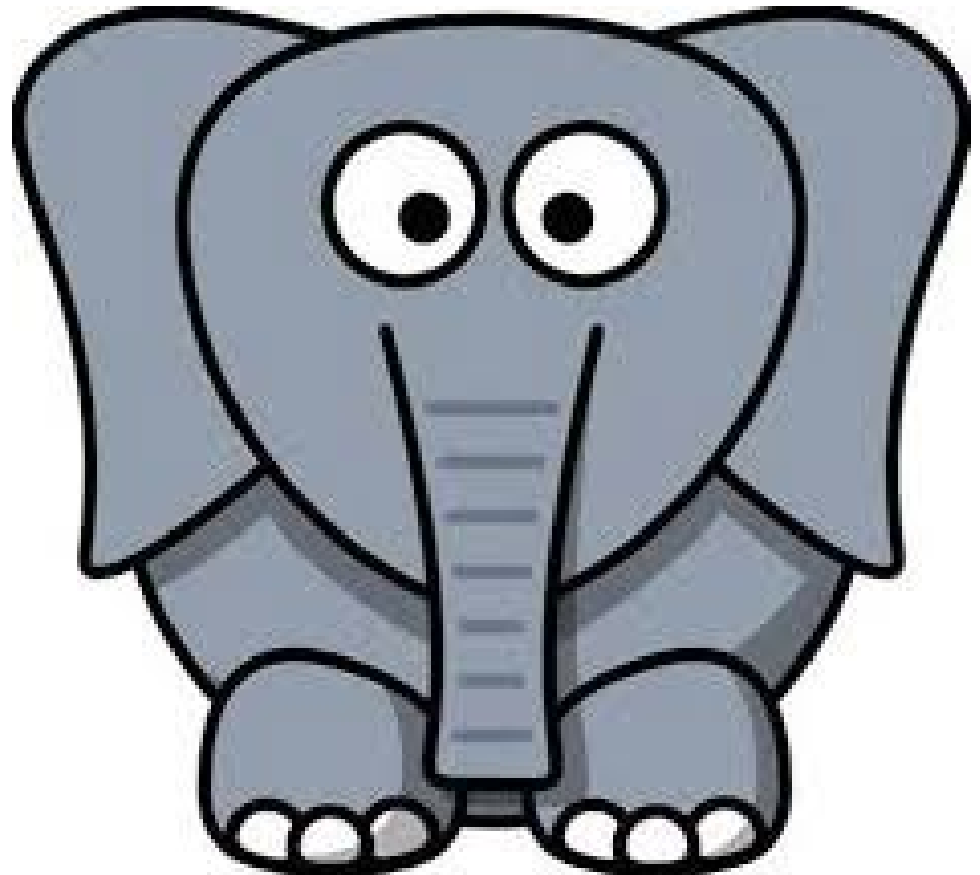
Privacy & Security Fundamentals

Data Privacy – the relationship between the collection and dissemination 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.

How do you analyze a data sharing issue?

One
bite at
a time



Analyzing a data sharing issue overview

1. Establish facts

- What
- Who
- Why
- How

2. Identify law and policy for both privacy and security

3. Apply law

4. Establish & document terms for sharing

Goal: Find and Support Pathways to Share Data



Attorneys are necessary to ensure that information sharing complies with laws

Cooperation: Getting to Yes!

Data Requester & Data Holder

- » **Come prepared with factual information**
 - The What, Who, Why & How
- » **This is what we want to do. . .**
- » **How do we best do it?**
 - Pathways to yes
 - Detour when needed
 - Minimizing risk
 - Judgment calls
 - For attorneys, there is safety in numbers! **Find out how similar projects reached “yes” on law.**

Diagramming **The WHAT** **The WHO** and **The HOW**

» **What is a “use case”?**

Use Case vs. Case Study vs. Hypothetical Scenario

» **Why is it important to clearly define your use case?**

» **Diagramming your use case**

OTHER Groups to include when working on use cases:

- » For research projects make sure to identify any relevant Institutional Review Board (IRB) that may need to review the proposal and potentially approve it
- » For any transfer, but especially electronic, make sure to consult with your agencies security team to ensure all appropriate precautions are taken and that both the method of transfer and endpoint are secure

(Continued next slide)

OTHER Groups to include when working on use cases (continued)

- » If you have received the data from another agency, consider whether you need to reach out for approval/clarification before redisclosing it
- » Internally, make sure to discuss among groups the approach to certain general categories of data in order to be as consistent as possible from project to project
- » If you are subject to FOIA, make sure nothing you are doing or saying is inconsistent with FOIA determinations on the issue of whether data is available to the public or if it protected

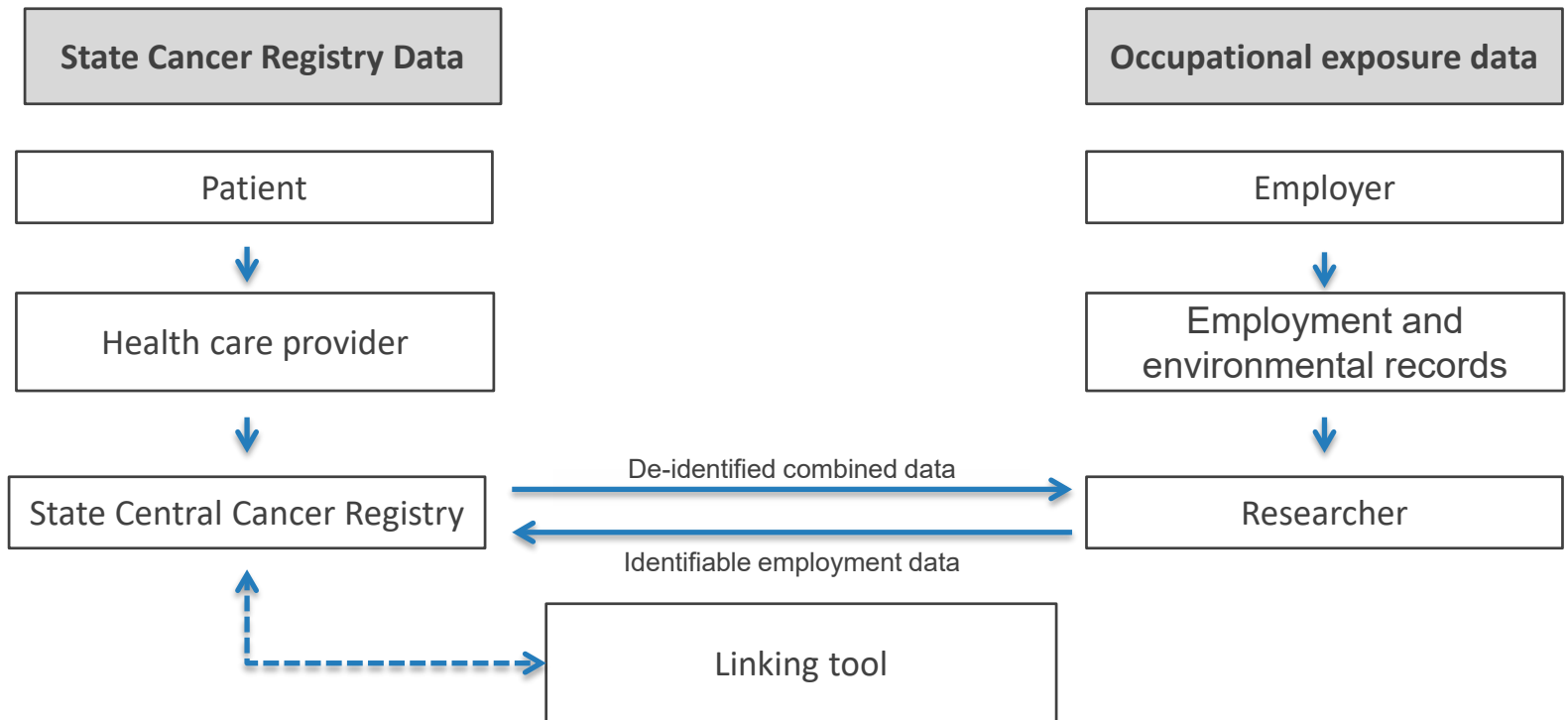
Diagramming your use case:

Simple: Data source 1 to a single entity for a single purpose.

Complex: Multiple data sources to a single entity for multiple purposes.

Map it!

Every transfer point for data is a decision point with regard to law



The WHAT

- » **What is the purpose of the request?**
- » **What do you want to do with the data?**
 - Individual (e.g. case management; care coordination; crisis intervention)
 - Systems (e.g. assessment and improvement; of individual organization or a services delivery systems (e.g. public health, health care, or human services)
 - Population health (e.g. surveillance, public health or community-level interventions)
- » **Consider in advance whether you might still be able to accomplish some of your goals even with a less granular level of data, if the more specific is not available.**

The **WHAT** (continued)

» **Consider what data, at a minimum, do you need to accomplish your goal?**

- Data Type
- Data Source
- Data elements
- Primary vs. secondary data use

Primary vs. Secondary Use of Data

for what purpose was the data provided?

for what purpose will the data be used?

Secondary use \neq second class

... But secondary use and disclosure **must be permitted** before using it for that purpose

- Permitted by law
- Permitted by review authority (e.g. IRB)
- Permitted by consent
- Are there any agreements, policies, or procedures that affect secondary uses?

What data do you need to accomplish your goal? (Examples)

Data Type	+ Data Source	→ Relevant Law
Health Care	Hospital	- HIPAA
Public benefit program	Substance use disorder program	- 42 CFR Part 2
Public Health Education	State agency	- FERPA
Claims	Local agency	- Public Health Code
	Federal agency	- State or federal administrative rules
	School	- Medicaid
	Individual	- Mental Health Code
		- Privacy Act

How much data do you need to accomplish your goal? (data elements)

- » Minimum necessary (If you collect it, you must protect it!)
- » When considering data elements, think about how this impacts the legal requirements depending on which elements you are requesting
- » Specific laws based on data element
 - e.g. Social Security Number Privacy Act
- » Degree of identifiability
 - Personally identifiable
 - Indirectly identifiable
 - Limited data set
 - De-identified
 - Anonymous

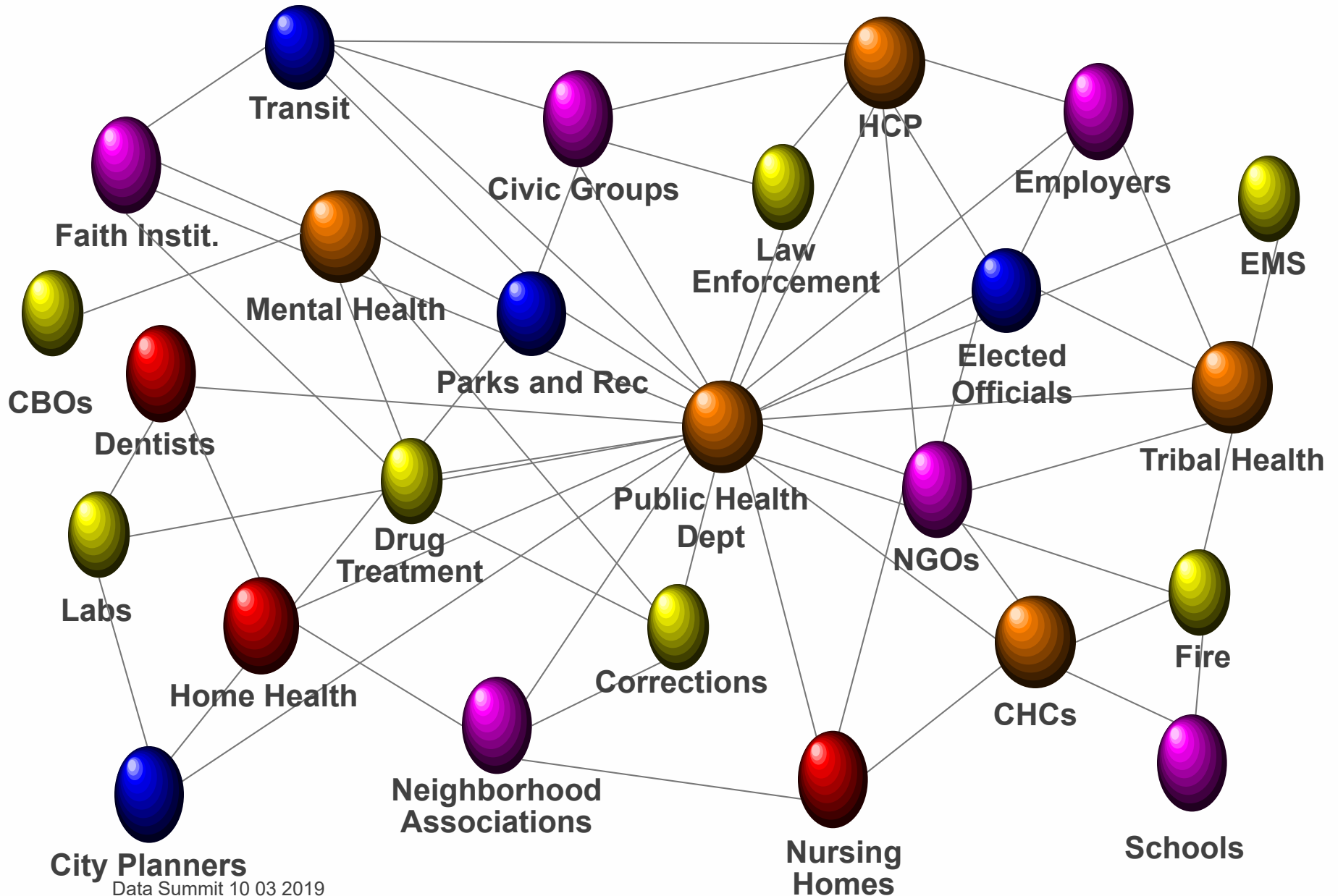
The WHO

- » **From whom might you obtain data; with whom do you want to share data? May be:**
- Among programs in one agency
 - Among agencies at one level or multiple levels of government
 - Among organizations in one sector or multiple sectors
 - Among public and private organizations

The WHO

- » **Public health leaders as Chief Health Strategists for their communities**
 - Public health special legal status - broad authority to collect data to prevent and control disease, protect public health, and promote wellness
- » **Multiple sector public and private partners**
- » **Health and nonhealth sectors**
- » **Partners that explicitly address "upstream" social determinants of health**

Local Public Health System



The WHO

- » **From whom might you obtain data; with whom do you want to share data?**
- » **Identify:**
 - **Each data provider** – name, type, characteristics, relationship between data provider(s) and data recipient(s)
 - **Each data recipient** – name, type, characteristics, relationship between data provider(s) and data recipient(s)

The WHO

Examples of type: public health agency, health care provider, substance use disorder provider (Part 2 program), educational institutional

Examples of relationship: Data provider-recipient programs within same health department

Examples of characteristics: HIPAA covered entity status, Part 2 Program, data covered specifically by state statute or rule

Use case diagram (covered earlier) helps to map parties, data flow, relationships

The WHO

Documenting relationships

- » Establish general terms of the relationship, secure commitment, e.g. partnership agreement, charter, or master data sharing agreement
- » Enter a data sharing/use agreement for a specific project
- » Reflect on-going initiative with master data sharing agreement – appendices to cover specific projects

The WHY (Purpose)

- » **Why are you sharing these data with these partners?**
- » **Permissible and prohibited disclosures often depend on purpose, be aware of allowable purposes to avoid delay or confusion**
- » **Be specific**
 - What is connection between data and what you want to accomplish?
 - Permissible and prohibited disclosures often depend on purpose
 - Ensure that the stated purpose is consistent with the described proposed use. Even if an appropriate purpose is posited, if the use is not consistent with that purpose it may not be allowable.

Now that you have your use case ...

THE HOW – How are you going to accomplish data sharing?

Technical

- ☐ HIE laws and security **Note: HIE laws may have consent provisions that relate to privacy**
- ☐ Ensure that you have a complete understanding of any electronic systems you may use
- ☐ Make sure any electronic systems or transfers meet your organizational security requirements, which should be based in part on legal requirements

Continued next page

THE HOW – Technical (continued)

- ☐ Read EULA and other similar agreements carefully. For example, many google services suggest data harvesting may occur. That may not be allowable for transfer or storage for certain protected data types.
- ☐ Ensure access controls are properly implemented
- ☐ Ensure, when required, encryption both at rest and in transit
- ☐ Ensure any user receiving data will adequately protect it and is not using any known vulnerable or inappropriate systems for data storage
- ☐ Consider why this is important (e.g. recent ransomware attacks)

Analyzing a data sharing issue

Identify privacy and security laws that apply to each

» **Data type**

» **Data source**

May include general and/or specific laws:

- Health information
- Public health data and reporting
- Medical records
- Data Practices
- Privacy
- Security
- Breach notification
- Sunshine laws
- Identity theft protection acts
- Patient rights
- Health professional or facility licensing, certification
- Insurance laws
- Consumer protection laws
- Health information exchange
- Social Security No. protection

Analyzing a data sharing issue continued

Apply law

- » **What does each law allow?**
- » **What prerequisites, conditions, limitations apply**

Balance: Maximize benefits, minimize risks

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

Analyzing a data sharing issue: Establish and document terms of sharing

- » Set out legal authority, terms for sharing, provides for monitoring and accountability for compliance with terms
- » Also use to describe relationship(s) between parties, project purpose and aims and how proposed data sharing furthers the purpose and supports the aim
- » Decide which type of agreement is appropriate (factors that are relevant to type of agreement)
- » **Bottom line:** through this agreement you want to demonstrate that proposed data sharing is legal under all applicable laws!!

Establish and document terms of sharing, cont.

Data sharing agreement common terms

- » **Parties**
- » **Purpose**
- » **Communications**
- » **Definitions**
- » **Data to be provided (elements, frequency, format, method of exchange)**
- » **Privacy and security requirements**
- » **Period of agreement**
- » **Termination**
- » **Boilerplate** (e.g. authority, entire agreement, severability, limitation on liability, no third party beneficiaries, governing law, etc.)

Making law work. . . .

Approaches & solutions

- **This may require that you revise your use case**
- **Consent (some consents have specific requirements, i.e. HIPAA and Part 2, and some may not be combined, mainly HIPAA in most cases)**
- **De-identification (make sure you understand what the particular deidentification standard is. HIPAA for example is very specific, but other state laws are more general and may depend on agency or entity policy)**

Making law work. . . .

Approaches & solutions, continued

- **Structuring relationships**
- **Re-defining problem / approach (e.g. 42 CFR Part 2 data – move to research project rather than public health surveillance)**
- **Technology – e.g. hashing, Massachusetts approach re opioids)**
- **Modifying HIPAA covered entity status (e.g. moving from fully covered entity to hybrid)**

Informed consent as a solution . . .
people just want to be asked

Concern: May not be easy to design or implement an informed consent process

Concern: reduce value of data

- Self-selection

- Justice – inclusion of under-represented and vulnerable groups

Concern: Need the population data for population health

Sharing data without consent

Navigating law

De-Identification



might be a key to open doors

- » **If remove or obscure personally identifying information in a dataset**
- » **Then most laws do not prohibit release of de-identified information**

De-Identification as a solution

“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

Concern: Sufficient identifiers needed to link and combine data across databases and data sources

Sharing Identifiable Data *without consent*

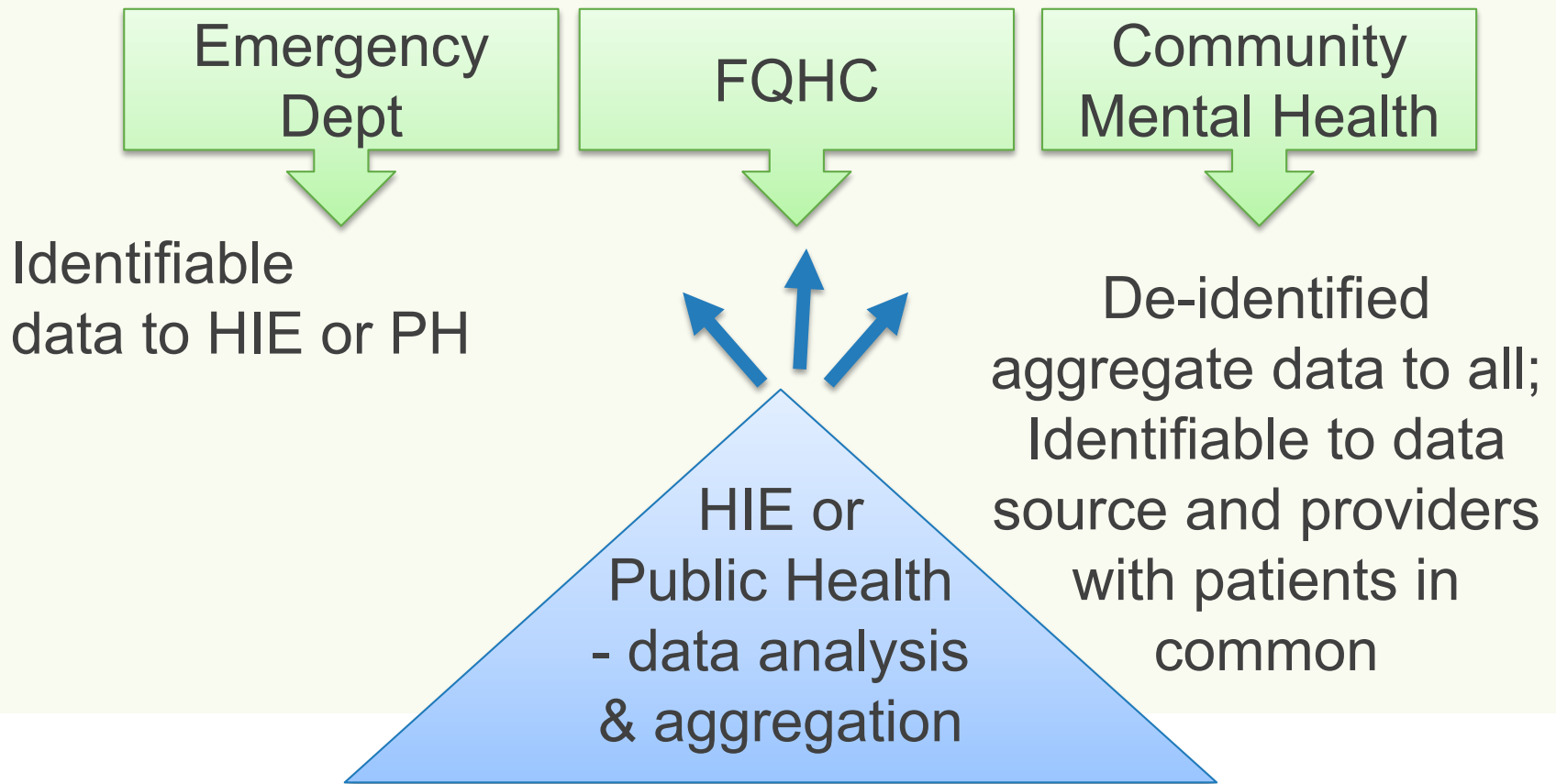
- Law provides for permissible uses and disclosures
- What does law allow?
- What are prerequisites, conditions and limitations?

Sharing Identifiable Data *without consent*

Possible solutions

- **Redefine project**
 - **E.g. Substance use disorder data (move from nonresearch project to research project)**
- **Structure relationships**

HIPAA: Identify high utilizers of various health care services to better address individual's needs



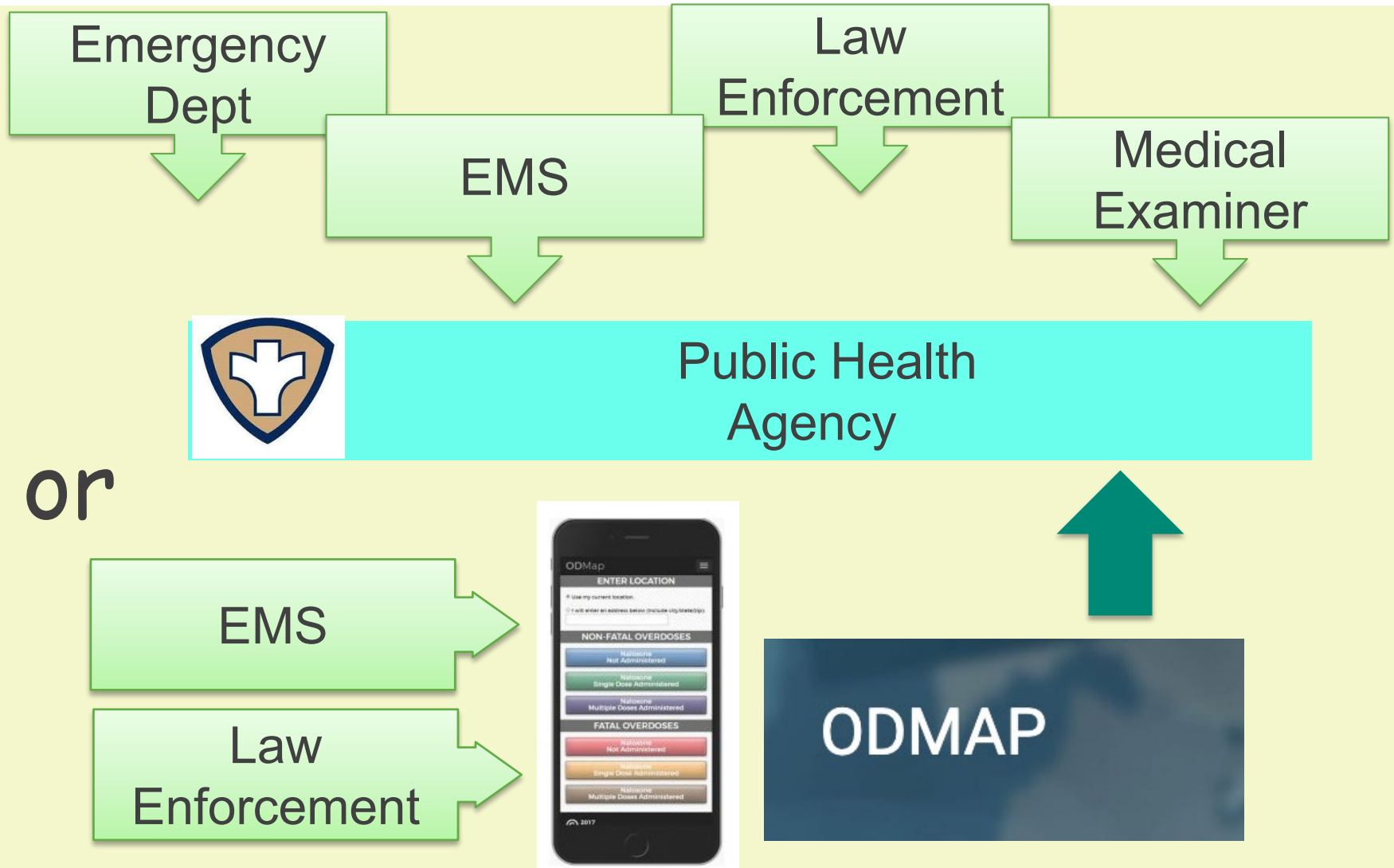
HIPAA: Identify high utilizers of various health care services to better address individual's needs

- HIPAA allows identifiable data to be shared with public health **authority** without authorization
- HIPAA allows identifiable data to be shared with a BA for data aggregation and de-identification; identifiable data may be provided to providers for patients in common for health care operations

42 CFR Part 2: Identify high utilizers of various health care services to better address individual's needs

- Part 2 requires consent for identifiable data (including LDS) to be shared with public health
- Part 2 allows a QSO to analyze, aggregate and de-identify provider's data – reports may be shared with other organizations. Part 2 does not allow QSO to combine identifiable data of multiple providers without consent, even for purposes of aggregation and de-identification
- Consider disclosure for research provided IRB/Privacy Board approves waiver of consent

Opioid Overdose Prevention



Sharing Identifiable Data
without consent

Family Educational Rights Privacy Act

FERPA

Obtain and use directory
information

Support School's
Mission: Student
Success

Data Summit 10 03 2019



Analyzing a data sharing issue: Establish and document terms of sharing

- » **Data sharing agreements & MOUs**
- » **Set out legal authority, terms for sharing, provides for monitoring and accountability for compliance with terms**

Establish and document terms of sharing, cont.

Data sharing agreement common terms

- » **Parties**
- » **Purpose**
- » **Communications**
- » **Definitions**
- » **Data to be provided (elements, frequency, format, method of exchange)**
- » **Privacy and security requirements**
- » **Period of agreement**
- » **Termination**
- » **Boilerplate** (e.g. authority, entire agreement, severability, limitation on liability, no third party beneficiaries, governing law, etc.)

Navigating Law to Share Data

Network for Public Health Law Resources

- **Checklist of Factual Information Needed to Address Proposed Data Collection, Access and Sharing to Improve the Health of Communities**
- **Data De-Identification Toolkit**
- **Federal Privacy Laws – snapshots + annotated compilation**
- **HIPAA Hybrid Status Toolkit**

https://www.networkforphl.org/resources/topics__resources/health_information_and_data_sharing/

Navigating Law to Share Data

Resources continued

Legal Bibliography



- *Data Across Sectors for Health*
- *Network for Public Health Law*

<http://legalbib.communitycommons.org/>

Thank you!

Denise Chrysler, J.D.

dchrysler@networkforphl.org

Colin Boes, J.D.

BoesC1@michigan.gov

