



AIRA
AMERICAN IMMUNIZATION
REGISTRY ASSOCIATION

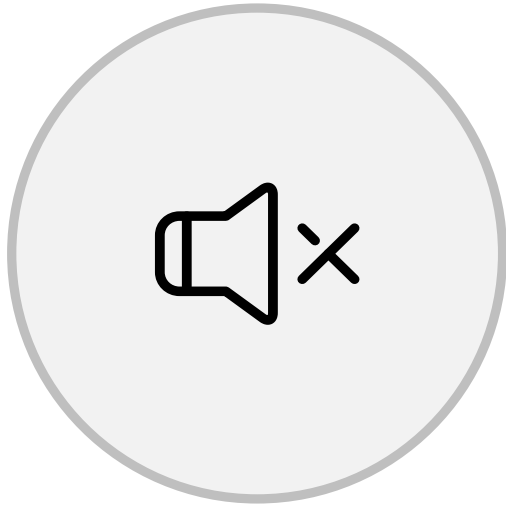
AIRA Discovery Session

Considerations when Developing IIS Policy

July 22nd, 2019

4pm ET

Welcome



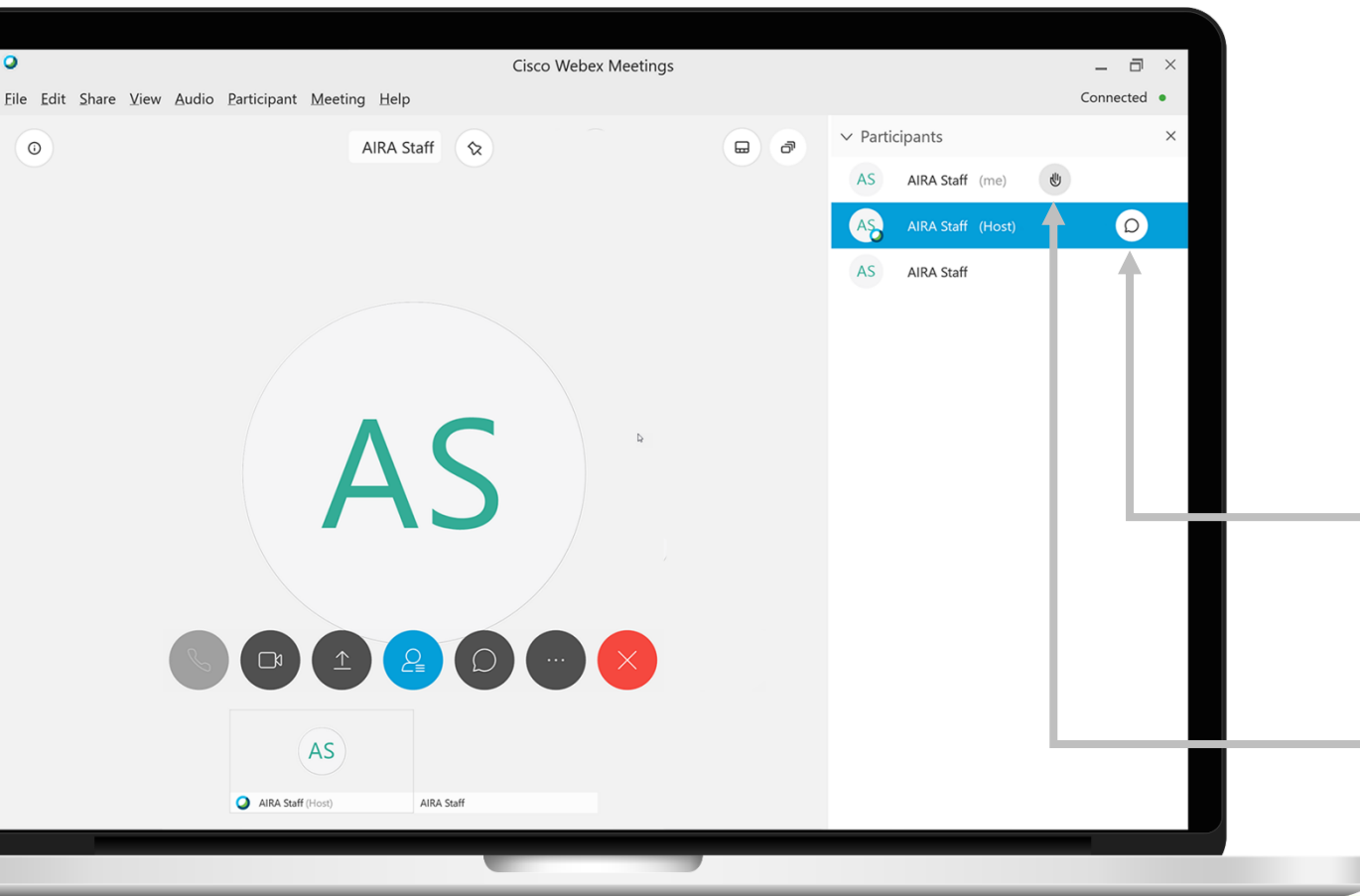
All phone lines
are muted



This meeting is being recorded
and will be posted on the
AIRA repository

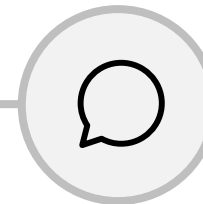


Welcome

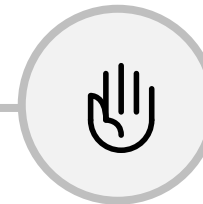


How do I ask a question?

- There will be time allotted for Q&A following the presentation, to unmute your line **press *6**
- Via WebEx:



Select the chat icon next to the host and type question into the chat box.



Select the hand icon next to your name and you will be called on.



Today's Topics

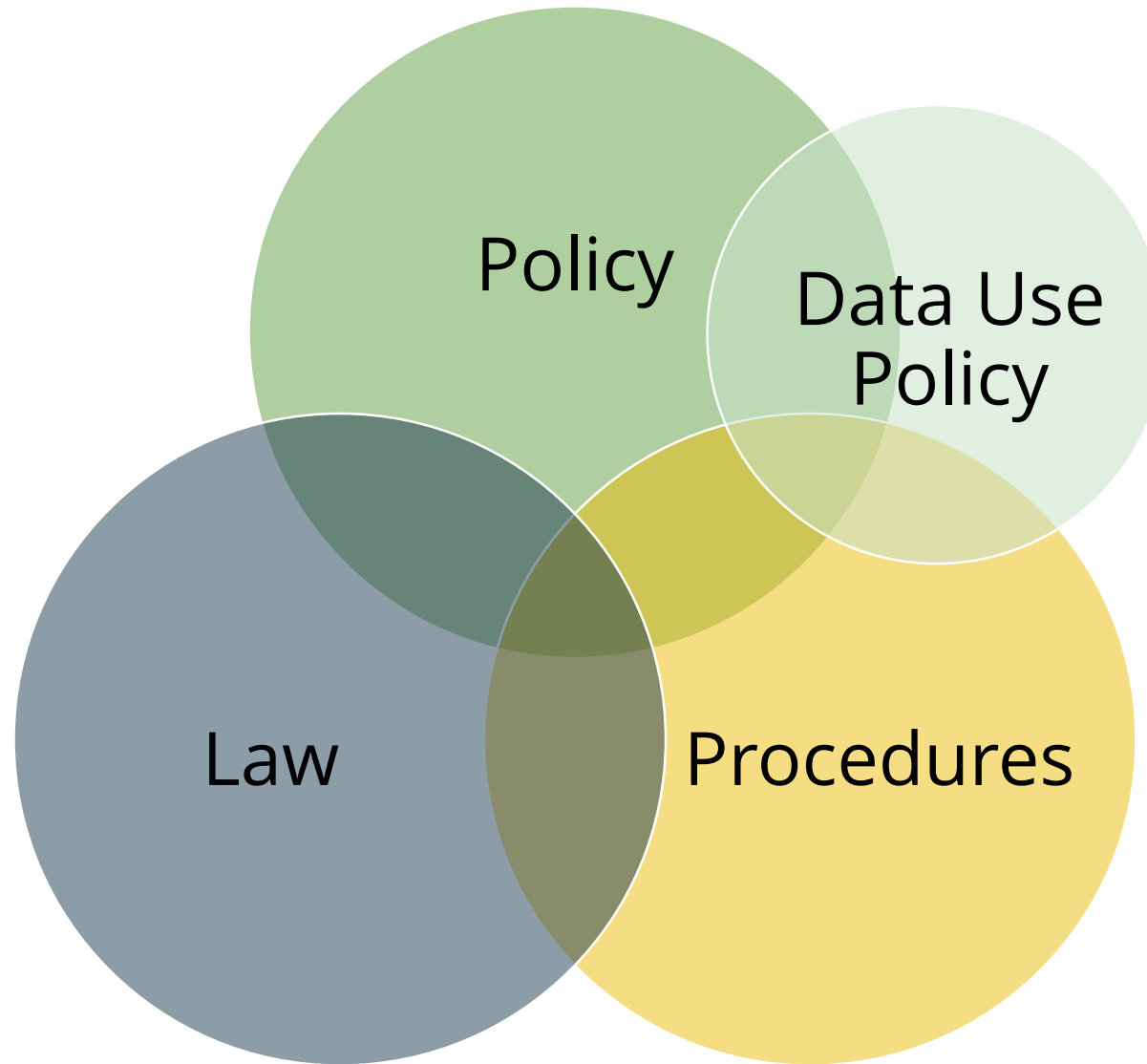
- What is currently happening across the IIS community re: policy documents?
- What key aspects should you consider when developing policy?
- What is the on-the-ground/in-the-wild policy experience?



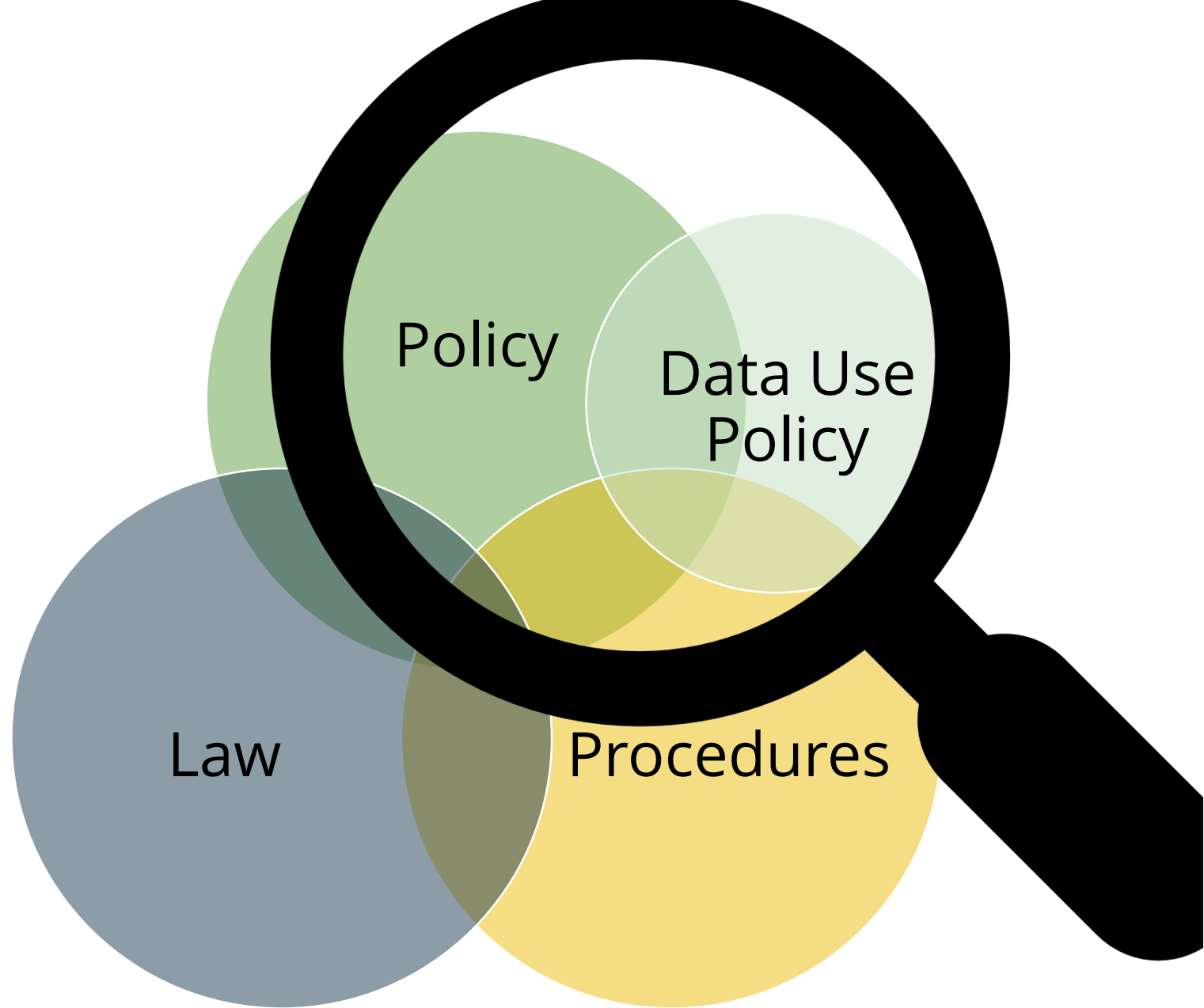
Press *6 to unmute your line



Scope



Scope



Today's Policy Landscape

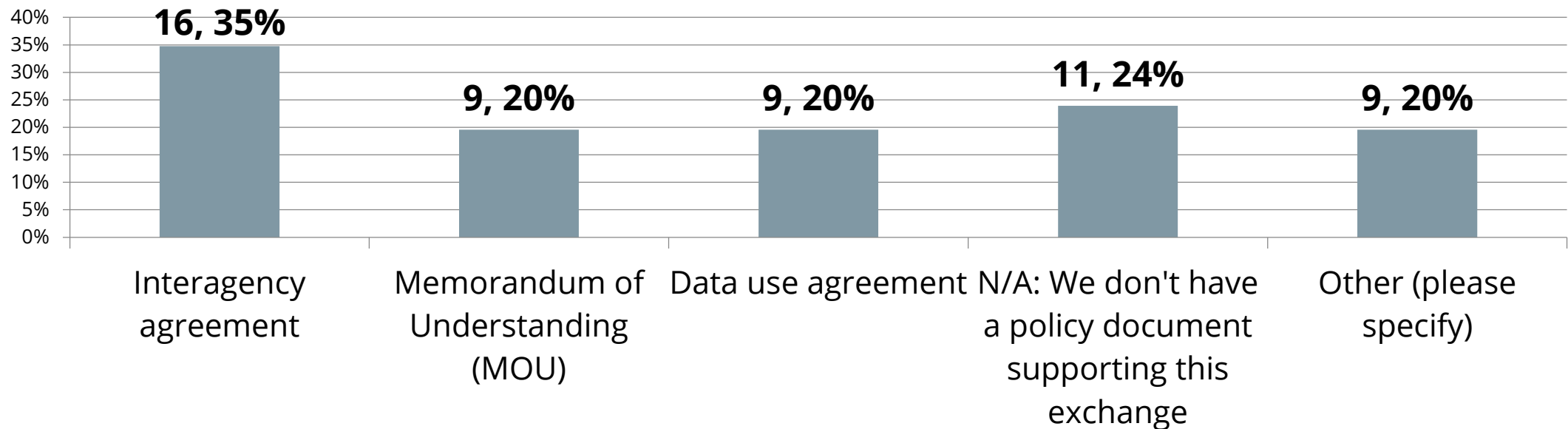
AIRA sent out a questionnaire to the IIS community on policy issues

- IIS programs were asked to submit one response per jurisdiction
 - 50 respondents (Thank You!) representing 50 unique jurisdictions
 - Questions asked what data exchange was actively happening, and what policy documents facilitated these exchanges
 - MUCH more detail will be shared at a session at the AIRA National Meeting



Results - Vitals

- 44 of 50 (88%) receive data from Vital Records
- Out of those 44 respondents, a variety of policy documents define the terms of data sharing

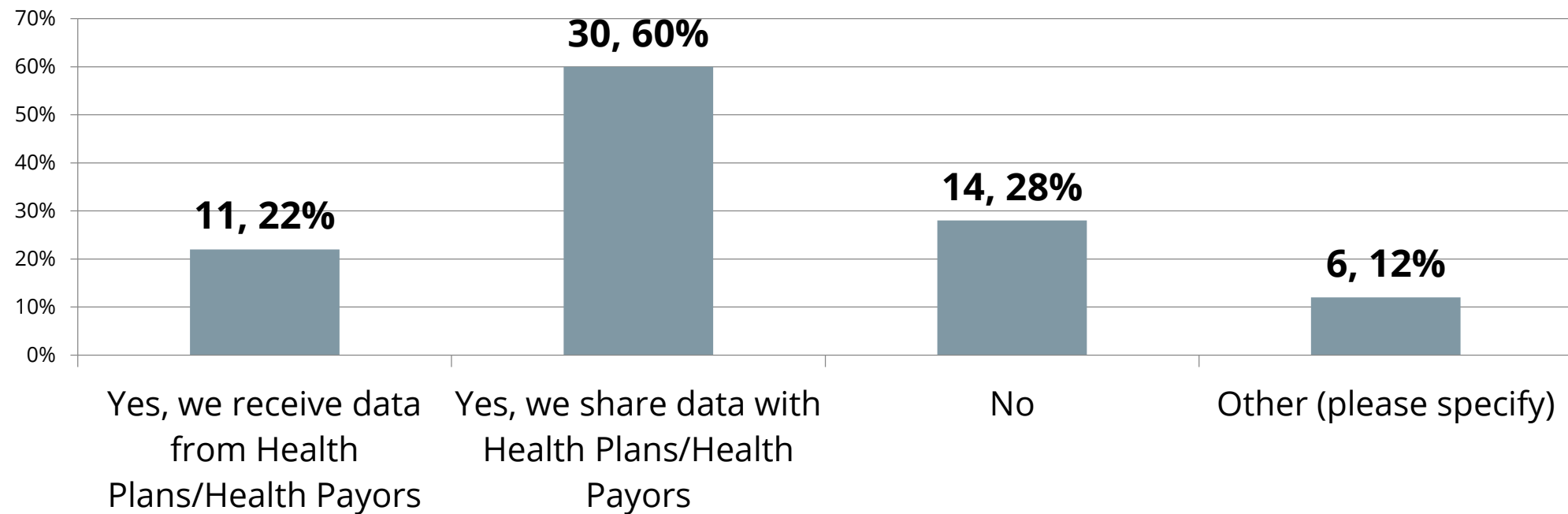


Note: Categories are not mutually exclusive



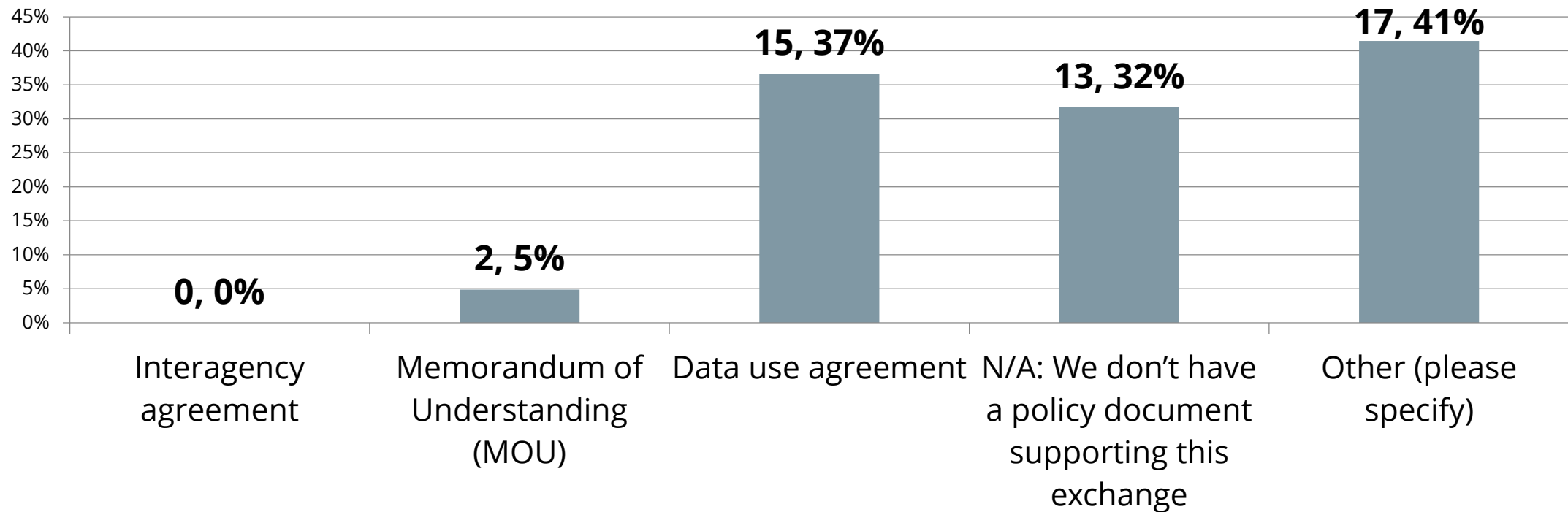
Results – Health Plans/Health Payors

Do you exchange data with Health Plans/Health Payors (check all that apply)?



Results – Health Plans/Health Payors

If yes, what policy document supports this exchange (check all that apply)?



Today's Speakers

- Jennifer Bernstein, JD, MPH, Deputy Director, Network for Public Health Law – Mid-States Region
- Heather Roth, Deputy Immunization Branch Chief, Colorado IIS Program Manager



Press *6 to unmute your line



IIS Policy Documents

Jennifer Bernstein, JD, MPH
Deputy Director, Network for Public Health Law
Mid-States Region

What is a law?

Law is a system of rules that are created and enforced through governmental institutions to regulate behavior by subjecting a party to criminal punishment or civil liability.

» **Statute**

» **Regulation / Administrative Rule**

» **Executive order**

» **Case law**

Law governs every aspect of data

Collection

Use

Sharing

Protection

Variation in Law Across Jurisdictions

All levels of government have the power to enact laws as well as different jurisdictions, such as federal, tribal, state and local governments. This allows for a great amount of variation in legal frameworks.

What is a policy?

A statement of intent, effectuating a deliberate system of principles, meant to guide decisions and achieve rational outcomes.

What is governmental policy?

Governmental policy outlines a government's goals and the methods and principles the government will use to achieve those goals. A governmental policy document is not a law but it will often guide the implementation of a legal framework to achieve governmental goals.

What is organizational policy?

The collection of mechanisms, processes and relations by which organizations are controlled and operated. Governance structures and principles identify the distribution of rights and responsibilities among different participants in the organization, including interactions with entities outside the organization. Policies also include the rules and procedures for making decisions in organizational affairs.

Role of organizational policies

- Provide general guidance about the organization's mission
- Provide specific guidance toward implementing strategies to achieve the organization's mission
- Provide a mechanism to control the behavior of the organization

Organizational policy documents

» **Memorandum**

» **Guidance documents**

» **Policy manuals**

» **Contracts and agreements**

- DUA
- MOU
 - Interagency agreement
- User agreement

What's in a name?

» **Data sharing agreement**

» **Data use agreement**

A legally enforceable agreement that operationalizes the (electronic) sharing of data among different parties, including organizations and individuals, while protecting data rights including privacy and confidentiality rights.

What's in a name?

» Memorandum of understanding

A legally non-binding agreement between two or more parties that outlines terms, scope and details of a mutual understanding, noting each party's requirements, roles, and responsibilities. It often avoids a lengthy contract review process and is therefore easier to execute.

Interagency agreement

- » An **interagency agreement** is a document, generally between government agencies and/or departments, that defines cooperative work between them
- » It is subset of MOUs specifically between two or more government agencies
- » May be easier to enter into than other types of agreements
- » Also be subject to state legal requirements and limitations in statutes, regulations, or guidelines

DUA vs. MOU

- » **Memorandum of understanding expresses a convergence of will and understanding between parties, indicating an intended common line of action**
- » **MOU most often is used in cases where parties do not intend to imply a legal commitment to each other, but do wish to engage in an agreement of principle**

General barriers to exchange

- » **State law applies – variation among states**
- » **General vs. specific authority to exchange data**
- » **Scope of sharing: prerequisites, conditions & limits**
- » **Within a state – applicability of multiple laws, need to harmonize**
- » **Variety and changing systems, manner of exchange, technological capability**

Develop a data sharing relationship

1. **Establish facts**
2. **Identify law**
3. **Apply law**
4. **Establish & document terms for sharing**

Your attorney should be a part of the team from the very beginning.

Determining exchange authority

1. Establish facts

- Data
- Participants
- Flow

2. Identify law

3. Apply law

4. Establish & document terms for sharing

Apply law

- » **What does 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**

Special Considerations for IIS

» **HIPAA covered status**

» **State law**

- Consent: affirmative, implied
- Opt-in, opt-out

Establishing and documenting terms of sharing

- » **Data sharing agreements & MOUs can share similar terms and provisions**
- » **Sets out legal authority, terms for sharing, provides for monitoring and accountability for compliance with terms**

DUA/MOU elements

» Parties

- » Name all known parties
- » Provide for the ability to add additional parties after initial agreement is operational

» Purpose

- » Articulate the overall purpose of the data sharing collaboration
- » Articulate each particular use of the data

The purpose of this Agreement is to provide MDH with data specified in this Agreement related to recipients of Minnesota Health Care Programs (MHCP) as necessary for communicable disease surveillance, control, and prevention. This data includes information on individuals that have been diagnosed with, or exposed to, communicable diseases reportable to MDH, as well as data on immunizations provided to MHCP recipients. Additionally, DHS needs access to the MDH Minnesota Immunization Information Connection (MIIC) system for the purpose of assessing immunization coverage levels for MHCP enrollees, and for quality assurance and quality improvement initiatives.

DUA/MOU elements

» Legal Authority

» General authority

» Specific authority

3. Data Source legal authority	
Citation	Description and detail regarding legal authority to collect, use and share the data, including limitations on use or disclosure of the data
Minn. Stat. 144.05, subdivision 1	The state commissioner of health has general authority under Minnesota Statutes, section 144.05 to conduct studies and investigations, collect and analyze health and vital data, and identify and describe health problems.
Minn. Stat. 144.211-144.227	<p>Section 144.213 within the Vital Statistics Act establishes the Office of Vital Records with the authority to promulgate rules (Minn. R. 4601) for the collection, filing and registering of vital records information and to maintain a statewide system of vital records.</p> <p>Section 144.225 specifies disclosure of information from vital records. Vital records data are public with the following exceptions:</p> <ul style="list-style-type: none"> 144.225, subd. 2: Demographic data on birth records is confidential data if a mother was not married to the child's father when the child was conceived nor when the child was born, unless the mother authorizes this data to be public. 144.225, subd. 2a: Health data (information from which an identification of risk for disease, disability, or developmental delay in a mother or child can be made) collected in conjunction with birth registration or fetal death reporting is classified as private data. 144.225, subd. 6: The named identity of a group purchaser collected in association with birth registration is nonpublic data. <p>Notwithstanding data classified as confidential, private, or nonpublic, the data may be released to the individuals and entities specified within section 144.225.</p>
Minn. R. 4601	
Minn. Stat. Chapter 13	Minnesota Statutes, section 13.05, subpart 5 requires a responsible authority to "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure." Work assignments of individuals in the MIIC Operations Unit reasonably require access to not public birth record data and this IDUA describes how that data will be made available.

DUA/MOU elements

» **Communications**

- » Publication and dissemination of results
- » Public disclosure of data, de-identification requirements
- » Communication standards between parties to the agreement

» **Definitions**

- » Any entities or elements that are unique to this data collaboration or require a definition for shared understanding
- » Terms used within the agreement that might not have a shared meaning or understanding across sectors
- » Naming conventions and standards for data elements

DUA/MOU elements

1. DEFINITIONS

“Agreement” means this Agreement.

“CDC” means the Centers for Disease Control and Prevention.

“De-identified immunization data” means any immunization data that does not identify nor provide a reasonable or ready basis to identify an individual.

“IIS Immunization Data” means demographics and immunization status of individual persons collected by IIS regardless of whether in the form of raw data or appearing in other IIS features and functions as described in Paragraph 7. Once an immunization record is entered into IIS, the record stored in the IIS database is IIS Immunization Data.

“IIS patient record” means the IIS Immunization Data for an individual.

“Immunization record” means any record regardless of source documenting the status of individual persons.

“Party” or “Parties” means either or both DOH and Provider/Plan.

“Provider-verified immunization record” means a valid record produced or verified by a health care professional or facility documenting the immunization status of an individual. To be valid, the record must be in writing, dated, and indicate the name of the health care provider responsible for administering or reviewing each immunization, or a unique stamp of the provider or facility at which the provider practices.

DUA/MOU elements

- » Data to be provided + description of data
 - » Elements
 - » Data provider, data recipient
 - » Frequency
 - » Format
 - » Method of exchange

9. Information to be provided. Each party will provide the IIS core data elements, incorporated by the CDC in its IIS Functional Standards, 2013-2017, provided: (1) the sending party collects and has the capability to provide the core data element, and is permitted by its law to share the core data element and (2) the receiving party has the capability and capacity to receive the core data element. Appendix A identifies core data elements that each party is able to provide to and/or receive from other parties. Any party may agree to provide or receive additional data elements, to further the purpose of this MOU, as set out in Appendix A.

Appendix A

In the table below, each party to this MOU identifies IIS core data elements and any additional data elements that it is able to provide to other parties and receive from other parties. Unless indicated otherwise, the IIS core data elements below are identical to CDC's list at <http://www.cdc.gov/vaccines/programs/iis/func-stds.html> - appB, as accessed May 20, 2015.

Core Data Element	Maryland		Jurisdiction B		Jurisdiction C		Jurisdiction D	
	Send	Receive	Send	Receive	Send	Receive	Send	Receive
Patient ID (previously listed as "Medicaid Number")	✓	Required						
Patient ID: Assigning Authority ID (i.e., owning source)	✓	Required						
Patient ID: Type (e.g., medical record number, IIS ID)	✓	Required						
Patient Name: First	✓	Required						
Patient Name: Middle	✓ if available	Optional						
Patient Name: Last	✓	Required						
Patient Alias Name: First	✓ if available	Optional						
Patient Alias Name: Middle	✓ if available	Optional						
Patient Alias Name: Last	✓ if available	Optional						
Patient Date of Birth	✓	Required						
Patient Gender	✓ if available	Recommended						
Patient Multiple Birth Indicator	✓ if available	Optional						
Patient Birth Order	✓ if available	Optional						
Responsible Person Name: First	✓ if available	Recommended						
Responsible Person Name: Middle	✓ if available	Optional						
Responsible Person Name: Last	✓ if available	Recommended						
Responsible Person Name: Relationship to Patient	✓ if available	Recommended						
Mother's Name: First	✓ if available	Recommended						
Mother's Name: Middle	✓ if available	Optional						
Mother's Name: Last	✓ if available	Recommended						
Mother's Name: Maiden Last	✓ if available	Optional						
Patient Address: Street	✓ if available	Recommended						
Patient Address: City	✓ if available	Recommended						
Patient Address: State	✓ if available	Recommended						
Patient Address: Country	✓ if available	Recommended						
Patient Address: Zipcode	✓ if available	Recommended						
Patient Address: County of Residence	✓ if available	Recommended						
Race	✓ if available	Recommended						
Ethnicity	✓ if available	Recommended						
Birth Facility Name	✓ if available	Optional						
Patient Birth State	✓ if available	Optional						
Patient Primary Language	✓ if available	Optional						

DUA/MOU elements

- » **Privacy and security requirements**
 - » Custodial responsibility and data stewardship practices
 - » Roles and responsibilities of the parties to agreement
 - » Permissible use, linking, sharing and disclosure
 - » Governing law – HIPAA, FERPA, 42 CFR Part 2, state law
 - » Policies and procedures for reporting data breaches or unauthorized disclosures

DUA/MOU elements

» Privacy and security requirements

6.2 Duties Relating to Protection of Information.

- (a) **General Oversight Responsibilities.** Each Agency shall be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of Protected Information collected, created, used, maintained, or disclosed. This responsibility includes:
- (b) **Training:** Ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed above, and
- (c) **Duty to ensure proper handling of information.** Each Agency shall ensure proper handling and safeguarding of Protected Information by its employees, subcontractors, and authorized agents. This includes ensuring employees and agents comply with and are properly trained regarding, as applicable, the laws listed above in paragraph 6.1.
- (d) **Minimum necessary access to information.** The collection, creation, use, maintenance, and disclosure of Protected Information shall be limited to only those individuals employed by each agency, or those employed by the subcontractors or agents of each agency, whose work assignments reasonably require access to the Protected Information, entities or individuals who are authorized by statute to gain access to the Protected Information, and entities and individuals given access by the express written direction or permission of both agencies.
- (e) **Information Requests.** Unless provided for otherwise in this Agreement, if either agency receives a request to release any Protected Information, the other agency must be immediately notified. The Agency whose data is requested will consult with the other Agency's Authorized Representative as to how to respond to the request. The response to the request shall comply with applicable law.

DUA/MOU elements

» Disposition of data

WA DOH and OR DHS agree to destroy all confidential information obtained under this agreement once the purposes of the project have been accomplished. Information which cannot be destroyed or of which destruction is not feasible shall be maintained in a secure environment. WA DOH and OR DHS agree to include compliance with these requirements as a requirement for contractors. Retention is pursuant to state archive laws that will dictate data disposal.

» Period of agreement

» Termination

11. TERMINATION.

- a. Either Party may terminate this Agreement effective as of the end of any calendar quarter, provided the terminating Party gives written notice of termination to the other Party at least 30 days before the end of the quarter.
- b. Either Party may terminate this Agreement for cause after the other Party has failed to cure a material breach, provided the terminating Party gives the other Party written notice of breach and provides at least 14 days for the other Party to cure the breach.

DUA elements (not likely MOU)

» Boilerplate

- » Entire agreement
- » Severability
- » Limitations on liability
- » No third party beneficiaries
- » Modification
- » Warranties

Thank you!

Jennifer Bernstein, JD, MPH
jbernstein@networkforphl.org

public health
I  **LAWYERS**

AIRA Discovery Session

Data Use Policies in Colorado

July 22, 2019

Heather Roth, MA

Deputy Immunization Branch Chief & CIIS Program Manager



COLORADO
Department of Public
Health & Environment

Outline

- Overview of current data use policies and documents
- Current data use partners and structures

Division-Level Policy Documents

1) Dataset Use and Research Statutory Authority document:

- Helps programs understand how CO statutes govern their activities
- Provides a framework for programs
- Describes program-specific statutory charge
- Describes program-specific statutory reporting, confidentiality and authorized disclosures
- Identifies instances when individually identifying data can be disclosed under Department's Public Health Authority
- Describes program-specific abilities to engage in research

Department: CDPHE
Division: DCEED
Program: Immunization
Authorization to: CDPHE, CDPHE contractors implementing the program, LPHAs
Dataset: Colorado Immunization Information System (aka Immunization Tracking System and Immunization Registry)
C.R.S.: 25-4-1705, 25-4-2403, 25-4-902, 25-4-905, 25-4-906, 25-4-910
C.C.R.: 6 CCR 1009-2

Statutory Charge

- Purchase and distribution of low or no-cost vaccines to health care providers serving children who might not be vaccinated because of inability to pay.
- Implement and communicate rules promulgated by the Board of Health including but not limited to required vaccinations, vaccination frequency, issuance of immunization records, and distribution of immunization information.
- Develop and provide to the Department of Education a standardized document regarding required and CDC Advisory Committee on Immunization Practices recommended childhood immunizations by age.
- Provide official certificates of immunization to schools, private physicians, and local public health agencies.
- Examine, audit, and verify the records of immunizations maintained by each school.
- Establish a joint policy on immunization data collection and sharing in consultation with other state departments.
- Provide assistance to schools with the analysis and interpretation of the immunization data.
- Collect, review, and record epidemiological information for infants, children and adults.
- Identify opportunities to create best practices and improve immunization in Colorado.
- Issue immunization records to individuals (i.e., a child's parent/guardian/consenting person).
- May access and assess vaccination status data and contact the individual that is the subject of the immunization record if an immunization is overdue, or control an outbreak or prevent the spread of a vaccine-preventable disease.
- Enroll infants in CIIS using birth certificate data.

Statutory Reporting, Confidentiality and Authorized Disclosure**Data Provided By:**

- Individuals, health care professionals, health care entities, vital statistics, LPHAs, schools, managed care organizations, hospitals, HCPF
- Individuals may opt out of CIIS and must be notified that they can opt out, and;
- Schools, licensed child cares, and colleges report aggregate immunization and exemption data, by antigen (separate from CIIS).

Non-individually identifying data can be disclosed.**Individually Identifying Data can be Disclosed under the Department's Public Health Authority:**

- To provide treatment;
- To entities that provide the individual health insurance coverage;
- To provide an accurate and complete immunization record for the individual;
- To a school in which such person is enrolled;
- To link CIIS data and vaccine inventory (if task force recommended);
- To the CDPHE contractor that is implementing or operating CIIS so long as this complies with state and federal confidentiality laws (e.g., HIPAA, etc.);
- CIIS data may be relevant to other task force recommendations such as improving LPHAs' ability to bill insurance carriers;
- To the extent necessary for the treatment, control, investigation, and prevention of vaccine-preventable diseases. Disclosure of PHI or PII will be the minimum amount necessary to accomplish the public health purpose. It may be necessary to share PHI or PII information with, and perform data linkage for entities that are statutorily authorized to receive the identifying information, such as LPHAs, the Laboratory Services Division or the CDC/other states for multistate outbreaks. Note that this is more likely to occur if there is an outbreak of a vaccine preventable disease and thus the activities move from the immunization statutes to the communicable disease statutes. Release of identifying information is the minimum necessary;
 - No DUA is required.
- It may be necessary to publicly release limited identifying information such as a press release that provides the age of a single case.
- It may be necessary to share individually identifiable information in the course of performing day-to-day programmatic duties, such as contracting for CIIS maintenance services; and
 - DUA is required.
- Data linkage may be necessary to perform the Department's public health duties. An example may be improved utilization of electronic health records. The standards above apply to any release of data; to receive data beyond the data that is reportable pursuant to statute or BOH rules:
 - A BAA or DUA is required to receive an external data set, including another CDPHE program's data set
 - Document whether CDPHE is the custodian or owner of the data, whether the information is proprietary and understand whether we will have to produce it for CORA; define CDPHE use (vast majority of the time the only authorized purpose is to perform the data linkage), and; set destruction date of external data set.

Ability to Engage in Research and Scope of the Program's Participation

Does statute, rule or programmatic history authorize or prohibit the program to engage in research?

- NA - statute and rule are silent.
- The Program has participated in a couple of studies related to improving immunization rates. The activities built upon existing public health authority to notify individuals when their immunizations were overdue. But for the study being broader in scope (contributing to general knowledge about the value of

reminder/recall interventions) and the CDPHE Program not being the lead site, the activities could have constituted public health practice and been performed as quality improvement under the Department's public health authority.

Can the program engage in human subjects research?

- Yes, if the research contributes to general knowledge to improve immunization, or treat, control, investigate or prevent vaccine-preventable disease that will benefit Coloradans.
- Please see the *Recommended Actions for all Public Health Programs Datasets and Research Participation* to determine if participation is appropriate.
- CDPHE IRB review and approval is required before any human subjects research study can be started.

Can Colorado immunization data be used in research?

- Permitted for CDPHE Immunization Program-only research (i.e., not involving research partners including other CDPHE Divisions) so long as identifiable information is not disclosed.
 - HIPAA authorization or waiver of authorization required for CDPHE staff to access the data as they are no longer acting under their public health authority.
 - IRB approval required prior to engaging in research.
- Non-identifying or coded data may be shared for multi-site research.
 - HIPAA authorization or waiver of authorization is required for CDPHE staff to access the data as they are no longer acting under their public health authority.
 - IRB approval is required prior to engaging in research.
 - Data linkage may be performed to the extent doing so furthers the statutory charge of the Program (data linkage alone may not constitute engagement; see [CDPHE IRB Policy 2.1](#)); however, the study will need to be designed so CDPHE staff serving as study personnel, obtain the external data (identifying), access immunization data, and code or otherwise make the data non-identifying.
 - Along with the authorizations identified above, a BAA or DUA governing the external data set is required and HIPAA authorization or waiver may be required for staff to access the external data set.
 - IRB approval required prior to engaging in research.
- Individually identifiable data cannot be released to research partners unless a HIPAA authorization is signed and notarized for each study participant.

Division-Level Policy Documents

2) Data Release and Linkage Policy and Procedures

- General responsibilities of program staff
- Colorado Open Records Act requests
- Requests for de-identified, aggregate or statistical data
- Requests for access to and use of confidential data
- Requests for data linkage
- Data that are reviewed in-house by an external party
- Engagement in human subjects research
- Shared list of data elements considered confidential by Department

Appendix A Confidential Data

Confidential information includes data elements or other information in various DCEED public health surveillance systems that could be used to identify an individual. When developing this list, the Department has considered U.S. Department of Health and Human Services requirements relating to uses and disclosures of protected health information (45 CFR 164.514(e)(2)), HIPAA Protected Health Information standards, Department policy and best practices related to data privacy and data security. Data elements or products that fall into this category include (but may not be limited to):

- Individual level data with or without identifiers
- Names
- Geographical identifiers smaller than a state; however, the first three digits of a ZIP code can be used if Bureau of the Census data indicates that there are more than 20,000 people in the ZIP codes that share the first three digits. When the geographic unit contains less than 20,000, the three-digit code can be changed to 000.
- Dates (other than year) directly related to an individual
- Dates (year) when it identifies an individual or group of individuals age 90 or over
- Phone numbers (if not publicly available)
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Uniform Resource Locators (URLs) and Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code or number assigned in research to code data
- Facility-specific data or statistics
- Facility names and codes
- Rare conditions or causes of death
- Aggregate data with small cell sizes (eg. one's or two's, or other program-specific suppression criteria)

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
Vital Records	Daily birth and death certificate data to IIS	Interdivisional MOU	<ul style="list-style-type: none"> • Registries and Vital Statistics Branch Manager • Deputy Immunization Branch Chief 	<ul style="list-style-type: none"> • Registries and Vital Statistics Branch Manager • Immunization Branch Chief 	Annual Initial MOU was reviewed by department's Legal Director
Communicable Disease	Query interface between IIS and electronic disease reporting system	Intra-divisional MOU	<ul style="list-style-type: none"> • Public Health Informatics, Reporting and Refugee Branch Manager • Deputy Immunization Branch Chief 	<ul style="list-style-type: none"> • Communicable Disease Branch Chief • PH Informatics, Reporting and Refugee Branch Manager • Immunization Branch Chief 	Annual Initial MOU was reviewed by department's Legal Director

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
Health First Colorado (Medicaid)	<ul style="list-style-type: none">• Medicaid enrolled provider data (for VFC program)• Medicaid-eligible children (for VFC program)• Medicaid immunization claims• IIS data to support HEDIS	Interagency Agreement covering various programs	Each public health program included in IAA drafts its own section in collaboration with their Medicaid partner program.	<ul style="list-style-type: none">• Health Department Executive Director• Medicaid Executive Director• State Controller	Annual, unless an amendment is necessary during 12 month agreement period

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
Women, Infants and Children	WIC client demographic data sent to IIS	Interdivisional MOU	<ul style="list-style-type: none">• WIC Program Director• Immunization Branch Chief• IIS Program Manager	<ul style="list-style-type: none">• Prevention Services Division Director• WIC Program Director• Disease Control and Environmental Epidemiology Division Director• Immunization Branch Chief	<p>Indeterminate</p> <p>Initial MOU was reviewed by department's Legal Director</p>

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
School-Based Health Centers	<ul style="list-style-type: none"> • SBHCs report data to IIS • IIS generates biannual adolescent immunization coverage rates for SBHC clients 	<ul style="list-style-type: none"> • Data Use Agreement • Statement of Work • Confidentiality Agreement 	<ul style="list-style-type: none"> • Privacy Officer • Health Services and Connections Branch Chief • Deputy Immunization Branch Chief • Apex Evaluation (Business Associate of SBHCs) 	<ul style="list-style-type: none"> • Health Services and Connections Branch Chief • Immunization Branch Chief • Apex Evaluation President • Apex Evaluation staff (Conf) • Deputy Immunization Branch Chief (Conf) 	<p>Indeterminate</p> <p>All DUAs are reviewed by department's Privacy Officer</p>

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
Child Fatality Prevention	<ul style="list-style-type: none"> Immunization data for infant deaths from IIS to Child Fatality Prevention System to improve the quality of data obtained through child fatality reviews 	<ul style="list-style-type: none"> Data Use Agreement Statement of Work Confidentiality Agreement 	<ul style="list-style-type: none"> Legal Director Privacy Officer Epidemiologist and Data Visualization Manager Deputy Immunization Branch Chief 	<ul style="list-style-type: none"> Violence and Injury Prevention - Mental Health Promotion Branch Chief Immunization Branch Chief Deputy Immunization Branch Chief (Conf) Child Fatality Prevention Program Staff (Conf) 	<p>Indeterminate</p> <p>All DUAs are reviewed by department's Privacy Officer</p>

Current Data Use Partners and Structure

Data Partner	Data Exchange	Document Type(s)	Document Drafters	Signatories	Review Frequency
Health Plans	<ul style="list-style-type: none"> Immunization claims to IIS IIS data to health plans to support HEDIS reporting 	Letter of Agreement	<ul style="list-style-type: none"> Deputy Immunization Branch Chief 	<ul style="list-style-type: none"> Health Plan Representative IIS Program Manager or designee 	<p>Indeterminate</p> <p>All LOA templates are reviewed by department's Legal Director prior to implementation</p>
Participating Providers and Schools	<ul style="list-style-type: none"> Immunization and/or demographic data to IIS 	Letter of Agreement	<ul style="list-style-type: none"> Deputy Immunization Branch Chief 	<ul style="list-style-type: none"> Provider/School Representative IIS Program Manager or designee 	<p>Indeterminate</p> <p>All LOA templates are reviewed by department's Legal Director prior to implementation</p>

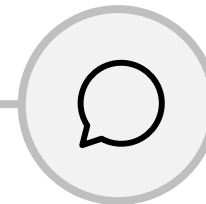
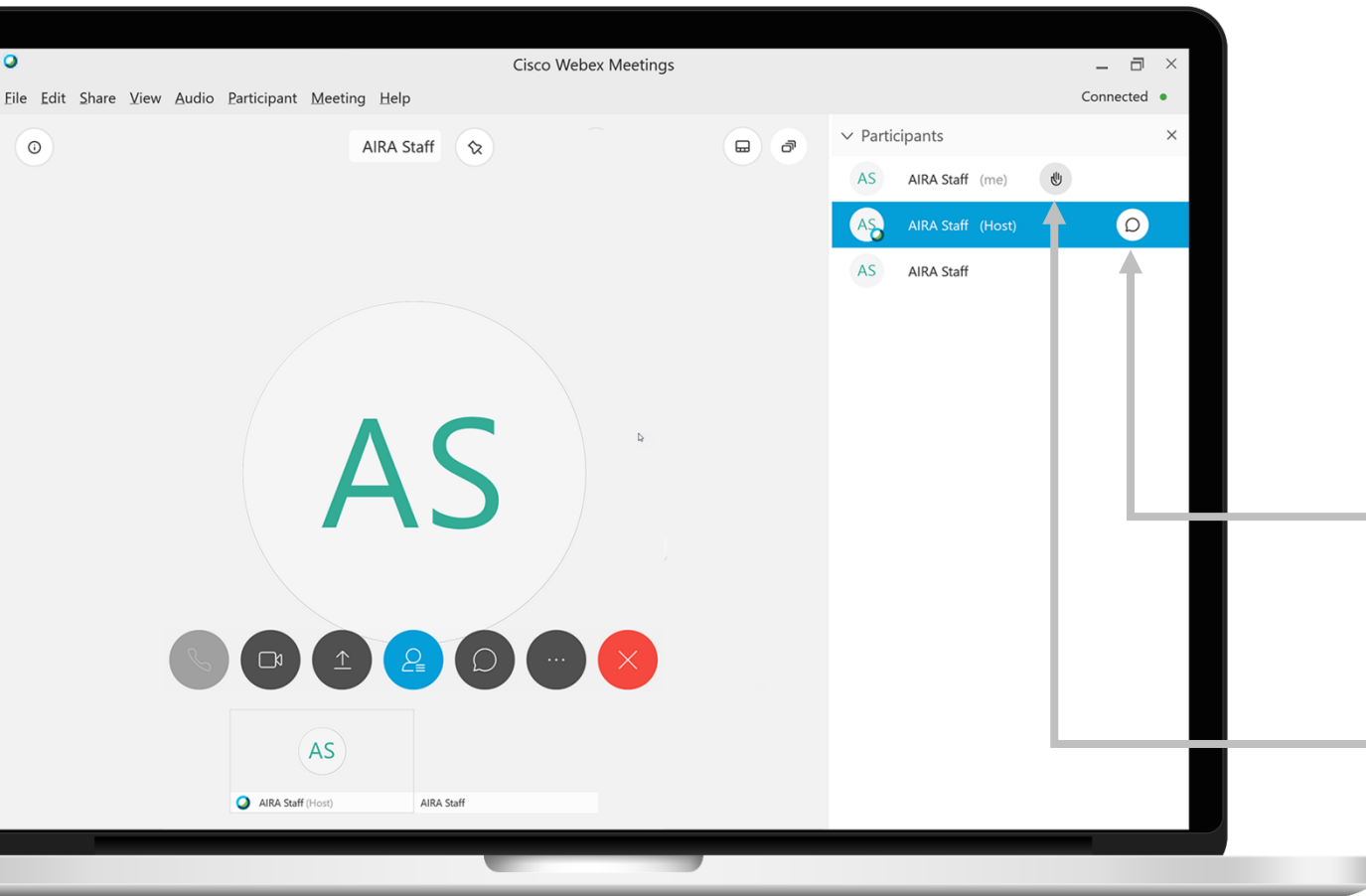
Questions, Comments, Discussion?



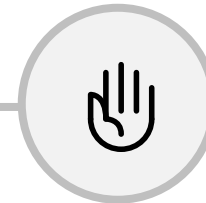
Questions, Comments, Discussion?

How do I ask a question?

- To unmute your line **press *6**
- Via WebEx:



Select the chat icon next to the host and type question into the chat box.



Select the hand icon next to your name and you will be called on.





Thank you to our presenters, and
thanks to all of you for joining us!

A brief evaluation survey will be sent out
following this webinar

The next Discovery Session will be August 26th at
4pm ET