The Network for Public Health Law

Ideas.
Experience.
Practical answers.

The Network for Public Health Law
Public Health Law Center
William Mitchell College of Law
875 Summit Avenue
St. Paul, Minnesota 55105
Tel (651) 695-7749 Fax (651) 290-7515
www.networkforphl.org

Memorandum

To: The Partnership for Public Health Law
From: The Network for Public Health Law[1]
Re: Legal issues related to cross-jurisdictional sharing of state immunization information system data
Date: December 1, 2014

I. Introduction

This memorandum discusses legal issues related to sharing state immunization information system data across state borders. State health departments must analyze their laws to determine that they have the legal authority to share data, to identify and comply with any limitations on sharing, and to ensure that sharing complies with federal and state privacy and security laws and maintains the trust of the community. For the most part, these laws are state-specific with variation among states in their terms and requirements. Cross-jurisdictional transmission and access are accomplished through a variety of methods, systems and infrastructure that are increasing in complexity with multiple points of data transfer. This memorandum presents five scenarios to illustrate variations, which raise common and different legal issues. Due to the variation in state laws and methods and systems for cross-jurisdictional sharing, this memorandum provides a four-step approach to facilitate legal analysis regardless of the state or structure for data sharing.

[1] The Network for Public Health Law developed this memorandum for the Partnership for Public Health Law. The Partnership is a collaboration of the American Public Health Association (APHA), the Association of State and Territorial Health Officials (ASTHO), the National Association of County and City Health Officials (NACCHO), and the National Association of Local Boards of Health (NALBOH). Individuals who contributed to the contents of this memorandum are: Denise Chrysler, JD, Director, Network for Public Health Law – Mid-States Region, Therese Hoyle, BSHE, Senior Public Health Advisor, Hoyle Consulting Inc., Public Health Informatics Institute and Michigan Department of Community Health, N. Elaine Lowery, JD, MSPH, Senior Public Health Consultant, Independent Consultant, Public Health Informatics Institute, and Jennifer Bernstein, JD, MPH, Senior Attorney, Network for Public Health Law – Mid-States Region. This memorandum is intended for informational purposes only and should not be considered legal advice. For legal advice, readers should consult their attorney.

II. Definition, Importance and Benefits of IIS

In 1997, President Clinton directed HHS to work with states to develop an integrated immunization registry system. As a result, the National Vaccine Advisory Committee (NVAC) launched an Initiative on Immunization Registries. NVAC outlined policy directions and major steps needed to establish a nationwide network of immunization registries while addressing four critical factors:[1]

1. Protecting the privacy of personal health information
2. Eliminating barriers to the current technical and operational challenges that states were experiencing
3. Ensuring patient and provider participation
4. Determining the resources needed to develop and maintain immunization registries

The federal, state and local immunization programs have made substantial progress over the past 18 years addressing these four areas. Today, Immunization Registries are known as Immunization Information Systems (IIS). Immunization Information Systems have been – and continue to be – key to maintaining and improving vaccination coverage and reducing vaccine preventable diseases in the United States. While IIS were originally created to benefit children, today most systems cover the whole lifespan.

An IIS delivers several services to the community in which it operates. It identifies populations at high risk for vaccine-preventable diseases. It also provides official immunization records to meet requirements for school, day care centers, employment, travel, and other purposes. It offers reminder recall functionality for healthcare providers and public health programs, allowing these organizations to generate and send immunization notices to individuals who are due or overdue for immunizations. It consolidates immunization information from various sources and exchanges immunization records with health care providers to ensure timely and appropriate administration of immunizations for their patients, thus decreasing the workflow burden on the provider office to locate immunization records from multiple sources.

Immunization Information Systems can be used to analyze important trends related to vaccination administration. IIS can help evaluate the uptake of new vaccines or show seasonal vaccination trends, such as influenza vaccines. These systems have become tools for immunization programs to support daily operations of managing vaccine supply, vaccine ordering, vaccine inventories, measuring immunization coverage rates by clinic, city, county or state, and managing outbreaks or pandemics during public health emergencies. They also provide the evaluation data for grant-funded activities, and the data to request grant funds to enhance immunization operations.

III. Importance and Benefits of Cross-jurisdictional Sharing of IIS data

There is growing demand for systems that enable efficient and effective sharing of public health data. IIS can serve as a model for the cross-jurisdictional sharing of public health data. Integrating the current IIS infrastructure to exchange information across federal, state and local jurisdictions will lead to more effective surveillance, better immunization planning and ultimately healthier communities. The goal is to establish interoperability among IIS that are capable of sharing information with other clinical health systems, including public health, while maintaining patient privacy and confidentiality.

The Health Information Technology for Economic and Clinical Health Act (HITECH),[2] part of the American Recovery and Reinvestment Act of 2009,[3] provides financial incentives to eligible healthcare providers that implement and meaningfully use certified electronic health record (EHR) technology. To qualify for stage 1 incentives, participating providers and facilities must meet one of three public health criteria. One available criterion is to test, and if successful, establish a connection from the EHR to the IIS in the provider's jurisdiction. This eliminates double data entry since information entered into an EHR automatically populates the IIS. As more immunization providers are using EHR systems, spurred by meaningful use requirements, IIS data will become more accurate and comprehensive.

A proposed objective in the CDC IIS Strategic Plan is that data exchange among immunization information systems is automatic and transparent regardless of location.[4] To this end, CDC has updated its functional standards for IIS to promote interoperability among IIS and the broader health information infrastructure.[5] Although they are not required, these standards are intended to improve vaccine delivery and guide the development of IIS by grantees that receive funding under 317(b) of the Public Health Service Act ("Section 317"). [6]

The benefits of cross-jurisdictional sharing of IIS data are extensive, including:

- Augmenting the reach of current IIS data uses by expanding population samples across jurisdictions
- Providing immunization records to providers for new patients who have relocated from another state
- Providing immunization records to providers who operate offices that border state lines
- Providing a comprehensive picture of vaccination rates for regional and national populations
- Tracking disease trends and treatment outcomes over time and across jurisdictions
- Supporting faster, possibly real-time, information exchange for public health decision making and management capacity

- Facilitating better public health coordination of vaccine preventable disease outbreak controls across state or jurisdictional borders

Immunization programs recognize the need to share immunization information across jurisdictional borders to serve patients who have moved from one jurisdiction to another, or who live in communities on borders as illustrated in the scenarios described in Section V below.

IV. Status of Cross-Jurisdictional Sharing of IIS Data

Forty-nine states, the District of Columbia, and three cities (New York, Philadelphia, and San Antonio) currently operate an IIS.[7] Although New Hampshire is not accepting immunization data at this time, it is in the process of establishing an IIS that is expected to accept data by early 2015. The New Hampshire Division of Public Health Services is working with healthcare providers, hospitals, and others to receive standardized immunization data from health care providers. That way, health care providers in the state can demonstrate "meaningful use" through electronic exchange of immunization data from a certified EHR system to an immunization registry.[8]

In 2012, the CDC conducted a study of laws, regulations and policies governing IIS in the fifty-three jurisdictions currently operating an IIS.[9] The study included legal authority to operate IIS for both children and adults, parental and adult consent for IIS participation, provider reporting requirements, authority for cross-jurisdictional sharing of immunization information, and other issues.

According to this study, for the jurisdictions that currently operate an IIS:

- Thirty-six IIS have the authority to share data with other jurisdictions. Twenty-nine of the programs responded that they do share data with other jurisdictions. These IIS share data either electronically via HL7 messaging, or flat file, or they allow providers who border their state access to the IIS via the user interface.
- Fifteen IIS do not have the authority to share data outside of their jurisdiction.
- Two IIS did not know if their IIS could share data outside of their jurisdiction.

For the 2012 survey, cross-jurisdictional sharing was broadly defined and included cross border sharing of information between providers and IIS. As shown by Appendix A, only a few states exchange data with other IIS. Appendix A summarizes the responses of Section 317 grantees in their 2011 IIS Annual Report (IISAR), to questions regarding grantee to grantee exchange of immunization information.[10]

V. Types of Cross-Jurisdictional Sharing of IIS Information

Cross-jurisdictional data sharing can occur in a variety of ways. Five scenarios, described below, offer examples of cross-jurisdictional data sharing using the IIS. Each scenario will be described in a generic framework. It will describe next steps for an immunization program to review the legal framework within their jurisdiction in order to manage cross-jurisdictional data sharing.

Many immunization programs collect immunization data from providers that are located in another jurisdiction. These providers are set up with access to the IIS for manual data entry. This type of data sharing is described in Scenario 1.

Scenario 2 describes cross-jurisdictional data sharing from IIS to IIS using a batch file upload. A batch file is an electronic file that includes more than one immunization record. These files may be submitted using a flat file or HL7 format. Some jurisdictions supply a batch file on a monthly basis to the bordering jurisdiction's immunization program. This allows the immunization program to collect data on residents who seek medical care across jurisdictional borders. It also assists with increasing population immunization coverage assessments in the IIS.

Scenario 3 describes the future of data sharing using HL7 real-time messaging between Immunization Information Systems. This process allows the provider to log into the IIS in their jurisdiction and search another IIS for a patient's immunization history.

Many immunization providers are moving away from manual data entry and toward automatic, real-time submission of immunization information from their electronic health record system to the IIS. Along with the increase of electronic health record adoption for many medical facilities, many states are expanding their health information exchange's (HIE) capacity with the goal of improving efficiency, and affordability, by transporting personal health data between private providers and public health. With implementation of the systems, the future of cross-jurisdictional data sharing will evolve between Health Information Exchanges and IIS. Described below are two HIE scenarios (scenarios 4 and 5) of how they may assist in the sharing of immunization data across jurisdictions.

A. Sharing Data Between IIS and Providers or IIS to IIS

Provider Accessing Bordering State IIS To Share Immunization Data

Scenario 1. State A has a children's specialty health clinic that sees many patients from the bordering state. Several hundred children who live in State B between the ages of birth to 18 years of age are patients of the clinic. The Children's Specialty Health Clinic would like to have access to State B's Immunization Registry. The IIS program in State B sends an IIS user agreement to the specialty clinic. The managing physician signs the agreement and sends it

back to the IIS program. The clinic is registered in the IIS and an on-line meeting is arranged to train staff how to use the IIS web page to query and enter data into the IIS.

To share data between an out of state provider and the IIS the following steps must be considered:

- Does state law permit the sharing of data across state lines?
- If the IIS receives vital records information does vital records allow the Immunization Program to share the demographic data with the provider in a different state?
- A data sharing agreement (IIS user agreement) will have to be signed by the requesting organization. What elements should be included in the agreement?
- Does the IIS collect school immunizations and can that information be shared with the clinic?
- Will this organization have access to all the reports in the IIS? Does a new role need to be created in the IIS for this type of access?
- Do the states' statutes/regulations require verification of a physician's medical license when enrolling them in the IIS? Does the immunization program have access to other state's licensing departments to fulfill this requirement?

IIS To IIS Data Sharing Using A Batch File

Scenario 2. A family lives in State A with their 5 year old, Jared. Jared gets immunizations from the long-time family pediatrician in State B. Periodically, the State B IIS checks to see if it has immunization information for any clients with a State A address and sends that information to the State A Immunization program. The Immunization Program uploads this batch file on a monthly basis. This update includes the immunization information for Jared from State A and this allows public health officials in State A to keep up with Jared's immunization status. This batch upload allows the State Immunization Program to access immunizations on residents that they would not have for the necessary population health reports, thus increasing immunization coverage rates for the State, and also for providers to access if Jared were to receive medical services in State A.

To share data between two IIS the Immunization Programs must consider the following steps:

- Does state law permit the sharing of data across state lines?
- What data elements may the IIS share with the other IIS?
- If the IIS receives vital records information does vital records allow the Immunization Program to share the demographic data with the other states IIS?
- A data sharing agreement will have to be developed between the Immunization Programs in these states to share immunization data with each other. What elements should be included in the agreement?

- Does the IIS collect school immunizations and can that information be shared with other jurisdictions?
- If the person has opted out of the IIS can you share that information with the other state's IIS?

IIS To IIS Data Sharing Using HL7 Real-Time Messaging

Scenario 3. A family moves from State A to State B with their 18 month old, Sara. Prior to the move, Sara received vaccines from a provider located in State A. Mom takes Sara to a new pediatrician in State B and tells the nurse that Sara got her immunizations in State A. The nurse logs into the State B IIS and hits the button "Search other IIS." The State B IIS contacts the State A IIS and gets Sara's immunization information to allow the pediatrician to order the correct vaccines. The current cross-jurisdictional data exchange between State A and State B is an HL7 query, and State A produces a real-time message back to the State B IIS with Sara's immunization history.

To share data between two IIS the Immunization Programs must consider the following steps:

- Does state law permit the sharing of data across state lines?
- What data elements may the IIS share with the other IIS?
- If the IIS receives vital records information does vital records allow the Immunization Program to share the demographic data with the other state IIS?
- A data sharing agreement will have to be developed between the immunization programs in these states to share immunization data with each other.
- If the person has opted out of the IIS can you share that information with the other state's IIS?
- Does the IIS collect school immunizations and can that information be shared with other jurisdictions?

B. Sharing Data with a Health Information Exchange

Laws, policies, mandatory reporting requirements and regulations related to health information exchanges should be reviewed thoroughly before an IIS program enters into a data-sharing agreement. Immunization Program Managers should have a liaison in the legal department review all data-sharing agreements between any and all other organizations and stakeholders (e.g., two departments in the same agency) that share data with an IIS, for example, lead screening, newborn screening, WIC, Medicaid, etc.

Health Information Exchange (HIE) is the electronic movement of health-related information among organizations according to nationally recognized standards.[11] HIE may also be used to refer to the organization that facilitates this exchange. HIE allows public health, health care

professionals and patients to appropriately access and securely share a patient's medical information electronically. There are many health care delivery scenarios driving the technology behind the different forms of health information exchange available today. While a single, national immunization information system with a consolidated database may be technically feasible it may not be politically feasible. The Comprehensive Child Health Immunization Act of 1993, as introduced, would have created a national immunization registry to follow the vaccination status of individual children. The proposal was derailed amid a firestorm of political protest.[12] Thus, rather than a national registry, the model for IIS became a nationwide network of community-and state-based immunization registries. This meant that each jurisdiction would develop its IIS with terms that reflect the politics and values of that community. In lieu of a national IIS, it may be feasible to facilitate nationwide IIS data sharing through Health Information Exchanges.[13]

One candidate for this network is the eHealth Exchange that emerged out of the Nationwide Health Information Network (NwHIN) interfaces, illustrated by the Michigan system below.

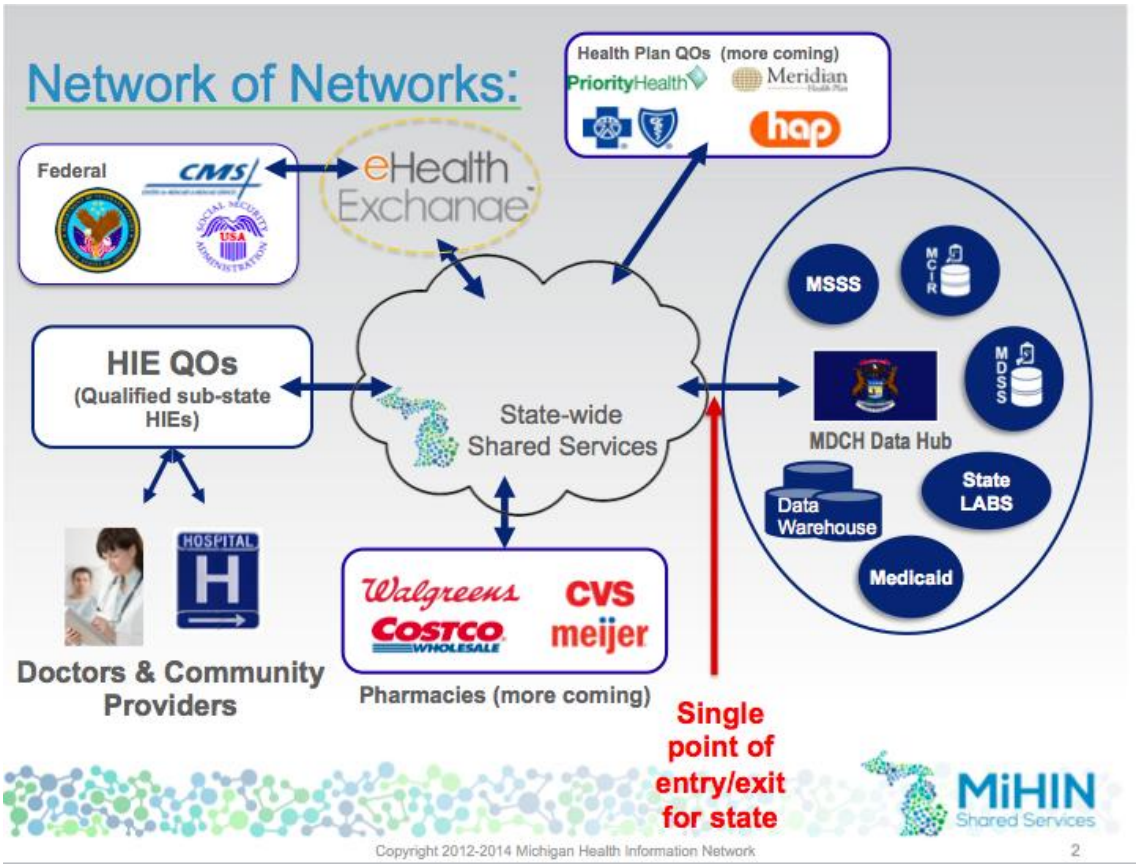


Figure 1 Michigan's Health Information Exchange Model

Under this model, the Michigan Health Information Network (MiHIN) serves as the point of entry/exit for the state. The MiHIN is a shared service that transports electronic health messages from healthcare organizations to the Michigan Department of Community Health in order to meet public health reporting requirements.

There is a data-sharing agreement or business associate agreement for every connection in the HIE infrastructure. As illustrated in the diagram above, MiHIN has agreements between all the entities that are connected to its shared services platform. Immunization programs should be prepared to ask questions about the legal issues that occur at every transfer point of the health information exchange.

Healtheway is a non-profit, public-private collaborative that operationally supports the eHealth Exchange (formerly referred to as the Nationwide Health Information Network Exchange). The eHealth Exchange began as the Office of the National Coordinator (ONC) nationwide health information network program in 2007. Since that time, a rapidly growing community of public and private organizations has been routinely sharing information. That community now represents thousands of providers and millions of patients. The eHealth Exchange now operates as an independently sustainable public-private community. Its purpose is to expand trusted, secure and interoperable exchange of health information across the nation by fostering cross-industry collaboration and by providing shared governance and necessary shared service to public and private organizations that wish to interconnect as a network of networks.[14]

New Initiative in 2014 for IIS Data Exchange

The Office of the National Coordinator for Health Information Technology (ONC) has launched a new immunization registry pilot program initiative. Participating pilot states will exchange immunization registry data through a data hub that will be developed by ONC. A list of pilot criteria has been established that includes, but is not exclusive to, the following:[15]

- IIS pilots must be able to support query response through bidirectional queries and must have a process to support acknowledgements
- State policy must allow immunization data to be shared across jurisdictions
- IIS must have a business need to exchange data with other participating states.

Public health departments are currently in different phases of working with health information exchanges. Many are in the planning stages of how data will be shared through the HIE and have concerns about privacy and confidentiality of the personal health information being shared. Common questions are whether an HIE is covered by the HIPAA Privacy Rule and whether an HIE can operate as a business associate of multiple covered entities participating in a networked environment.[16] These are discussed in Section VI F below.

Immunization Data Sharing between two Health Information Exchanges

Scenario 4. Every winter the pharmacies in southern states offer influenza vaccine to many retirees from the northern states. The pharmacies participate with the IIS in these states. One of the southern states has an operational HIE and has developed a use case to manage cross-jurisdictional data sharing of immunization messages from the IIS, and has signed business associate agreements with many of the northern states HIE's. The "go live" date to allow the sharing of immunization data will begin on October 1.

To receive immunization information from another state's IIS through an HIE the following steps would have to be considered:

- Does the Immunization Program have a business associate agreement with the local HIE?
- Does the Immunization Program have a policy that requires the identity of the source (where the data originated) to determine if an organization has the authority to submit immunizations to the IIS? The Immunization Program will not have user agreements with every provider in another jurisdiction. The Immunization program will have to determine if the HIE or the other state's IIS would become the source of origin of data being shared in this scenario.
- Does the Immunization Program have a data sharing agreement with the other state's IIS if identified as the owner of the immunization data?
- Does the IIS law allow the Immunization Program to receive data from an organization outside its jurisdiction?
- If the person has opted out of the IIS can you share that information with the other state's IIS?
- Does the IIS collect school immunizations and can that information be shared with other jurisdictions?

Federated Data Hub Service sharing Immunization data between IIS

Scenario 5: The IIS program would like to query patient records from bordering states' IIS through a federal data hub record locater service. Health and Human Services at the federal level has developed a data hub that can route the immunization messages between IIS. The IIS has signed a business associate agreement with HHS and is ready to test HL7 query messages from other state IIS.

To query data from another IIS through the Health Information Exchange the following steps must be considered:

- Does the Immunization Program have a data-sharing agreement with the other States' IIS?
- Does state law permit the sharing of data across state lines?
- What data elements may the IIS share with the other IIS?
- If the IIS receives vital records information does vital records allow the Immunization Program to share the demographic data with the other state IIS?
- If the person has opted out of the IIS can you share that information with the other state's IIS?
- Does the IIS collect school immunizations and can that information be shared with other jurisdictions?

VI. Application of Law To Cross-jurisdictional Sharing of IIS Data

Jurisdictions that want to exchange data should consult with their attorneys and/or privacy officers to determine legal authority and prerequisites, conditions, and limitations on sharing. Predominately, state laws apply. These might include state constitutions, statutes, regulations, and written policies adopted by states to implement their legal authority. Any court opinions or Attorney General Opinions interpreting law must also be considered. The following describes common types of laws that might apply, although the list is not exhaustive for all states. These range from laws specific to an IIS to laws that govern types of data stored in an IIS to laws that apply more generally to health information or data held by public health or other governmental agencies. Laws that govern infrastructure to transmit information, such as HIEs, might also apply. For multi-jurisdictional exchange, laws of both states that transmit information and states that receive information must be considered.

A. State Laws Authorizing IIS

The first step in determining if the Immunization Information System has the legal authority to share immunization data across state lines is to review state laws that authorize IIS. Authority to establish an IIS can be based on specific laws or policies or can be inferred from general public health powers. Do these laws allow, require, or limit sharing of immunization information?

Over the last decade, states have increasingly adopted specific laws authorizing IIS. According to CDC's 2012 study, for the fifty-one jurisdictions that operate an IIS that collects information on children,[17] thirty-six have specific laws that authorize operation of an IIS. With regard to adults, CDC reports that twenty-seven jurisdictions have specific laws that authorize operation of a life-long IIS. The remaining jurisdictions have laws authorizing the sharing of immunization information or general health information, or rely on general public health authority to operate

an IIS. Appendix B identifies jurisdictions that operate IIS based on specific authorization, immunization information sharing authority, health information sharing authority, and general public health powers.

Oregon and Michigan are examples of states with laws that specifically authorize establishment of an IIS and provide for cross-jurisdictional sharing of IIS information. Oregon Revised Statutes authorize exchange of information with other immunization registries, including out-of-state registries.[18] Administrative rules provide: "The manager [of the statewide immunization registry or his/her designee] may receive information from other registries and may share information with other such registries, provided that the manager makes a determination that other registries have confidentiality protection at least equivalent to those under ORS 433.090 through 433.102 and these rules. The manager shall prescribe the information that may be shared and the forms for sharing information to and from other registries."[19]

Michigan's Public Health Code requires that the Michigan Department of Community Health (MDCH) establish a registry to record immunizations and authorizes it to adopt rules regarding acquisition, maintenance, and dissemination of information contained in the registry.[20] Michigan administrative rules provide specific authority to exchange IIS information with another IIS. The authority is limited to information related to residents of another state or country.

> Rule 8. By written agreement, the department may transmit transcripts or copies of public health records or reports to state or national secure public health data systems or individuals responsible for the health care of a person if the records or reports relate to residents of other states or countries. The agreement shall require that the transcripts or records be used only for public health purposes and that the identity of a person who is subject to the report is confidential and shall only be released as specified in the agreement.[21]

While granting authority to exchange information with other state IIS, Michigan illustrates a pre-requisite (written agreement) and a potential limitation (records must "relate to residents of other states or countries"). This could impact Michigan's transmission of information regarding its residents who receive treatment in other states, such as those who live near a state border, to state IIS in those bordering states. Michigan's IIS could receive and incorporate information about its residents from other states (Scenario 2 above). Out-of-state providers could also be enrolled users in Michigan's IIS and report and access immunization information about their patients who reside in Michigan through Michigan's IIS interface (Scenario 1 above).

State laws and policies differ concerning who can access IIS information. For example, in some jurisdictions only health care providers who are licensed to administer vaccinations are

authorized to access information in the jurisdiction's IIS. Other jurisdictions specifically list persons and entities that can access the information in the IIS. The list of persons and entities can include (or not include): individuals/guardians, health care professionals, hospitals, pharmacies, schools, day care, WIC, Medicaid, military, Tribal, health information exchanges, researchers, and other IIS. In contrast, some jurisdictions do not have laws related to access of information in the IIS. In these cases, they may rely on general public health authority and policies interpreting the general public health laws. Some jurisdictions may allow full access to all authorized users, while other jurisdictions may allow read-only access to certain users.

State law must also be reviewed for consent requirements for including an individual's immunization data in an IIS to ensure that cross-jurisdictional sharing complies with the scope and any terms of consent. In its 2012 study, CDC reports that three states require that a parent or adult explicitly consent ("opt-in" model) to inclusion of information in an IIS: Texas, Kansas, and Montana. An additional four states do not require explicit consent for children, but require such consent for adults: Arizona (when adults are vaccinated by providers other than pharmacists), Arkansas, New Jersey, and New York. Some states allow the individual or parent to exclude their immunization data ("opt-out") whereas other states do not allow for exclusion. Appendix B identifies consent models for children and adults for each jurisdiction that operates an IIS.

B. State Authority During Emergency

In addition to routine sharing, states should identify laws that would apply during an emergency that impacts access to immunization information. Most jurisdictions have "emergency powers" that can be invoked to authorize data- sharing during emergencies. Some IIS used emergency powers to allow access to IIS information following Hurricane Katrina. Within days after Hurricane Katrina in September 2005, the Houston-Harris County Immunization Registry was connected to the Louisiana Immunization Network for Kids Statewide. This linkage provided immediate access to the immunization records of children who were forced to evacuate the New Orleans, Louisiana, area. 18,900 immunization records were found, representing an estimated cost savings of more than $1.6 million for vaccine alone and $3.04 million for vaccine plus administration fees.[22] Emergency powers allowed this data-sharing activity to occur, but after the emergency powers event ended, the data- sharing stopped between Louisiana and Houston.

C. Laws governing varying sources of information in an IIS

IIS contain information from a variety of sources within and outside the health department responsible for the IIS. These may include vital records, newborn screening, health care providers, pharmacies, schools, and Medicaid and other health care payers. Data from each of

the data sources may be subject to different state and federal laws. In most states, information in vital records is subject to specific confidentiality requirements and may retain some of those protections after incorporation into an IIS. Medicaid data is subject to applicable federal laws and policies, as well as state confidentiality policies. Interpretation of applicable federal laws and policies may differ among state Medicaid programs. Disclosure of education records held by schools may be subject to the Family Educational Privacy Rights Act (FERPA); as discussed below, FERPA prohibits re-disclosure of certain identifiable information absent a parent's consent. Laws that govern the source of each data element to be exchanged must be reviewed to ensure that cross-jurisdictional sharing is allowed.

D. State privacy, security, and confidentiality protections

State laws should be reviewed that govern public health information in general, including privacy, confidentiality, security, and data practices laws. These laws may protect the confidentiality of information in an IIS and prohibit unauthorized disclosures. States have increasingly passed laws that cover security of electronic information held by the public and private sectors including identity theft protection laws and data breach notification laws.

E. Laws regarding transport of data to and from the IIS

Technological advances for transfer of IIS information may implicate additional laws, such as laws specific to Health Information Exchanges. Idaho is trying to amend existing law to revise terminology and modernize the statute governing data use in the IIS to bring it into sync with current health information exchange practices and registry objectives. Some of the proposed changes are to allow the IIS to exchange data bi-directionally with provider Electronic Medical Records and to allow the IIS to utilize Health Information Exchanges (e.g. Idaho Health Data Exchange).

Some states have enacted laws requiring patient consent to include or transmit their health information through health information exchange. For example, Nevada's law states that a patient may not be compelled to participate in an HIE. Opt-in and opt-out consent models apply, depending on the type of information to be transmitted.[23] Similarly, Massachusetts requires that providers that connect to the statewide HIE establish a mechanism to allow patients to opt-in to the health information exchange and to opt-out at any time.[24] When enacting HIE consent laws, states need to avoid laws that would create barriers to transmission of immunization information to the IIS through HIE.

F. Federal Laws

While state law primarily determines legal authority to exchange IIS information, federal privacy, confidentiality, and security laws may also apply. Two federal laws establish national standards for the disclosure of identifiable information: the federal Privacy Rule,[25] adopted by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA)[26] and the Family Educational Rights and Privacy Act (FERPA).[27] HIPAA should not impact cross-jurisdiction exchange of information among providers or IIS. FERPA could affect sharing of certain information that originated from a school.

Health Insurance Portability And Accountability Act Of 1996 (HIPAA)

The HIPAA Privacy Rule sets a minimum national standard for protecting the privacy and security of individually identifiable health information ("protected health information" or "PHI"). The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and most health care providers ("covered entities"). It prohibits disclosure of an individual's PHI unless the individual authorizes the disclosure or an exception applies. HIPAA allows health care providers to disclose immunization information, without the patient's authorization, for purposes of treatment, as required by state law, or as authorized to a public health agency for the purpose of preventing or controlling disease, injury or disability including but not limited to public health surveillance, investigation, and intervention.[28] Under one or more of these exceptions, health care providers are authorized to submit patient information about immunization to an IIS without the patient's consent.

IIS are commonly recognized as public health entities. As such, they may not be strictly covered under HIPAA. Even for IIS that are covered by HIPAA, HIPAA should not interfere with cross-jurisdictional sharing. Forty-five per cent of IIS report that they are HIPAA covered entities.[29] The HIPAA public health exemption would allow covered IIS to share immunization information with other IIS, without an authorization, for the purpose of preventing or controlling disease, injury or disability. HIPAA would also allow covered IIS to share immunization information with providers for treatment purposes, whether the provider is located in the same or different state. While HIPAA should not interfere with cross-jurisdictional sharing of immunization information, if state law would not allow sharing, state law would control. The HIPAA Privacy Rule defers to state laws that provide greater privacy protections to the individual.[30]

Whether or not HIPAA applies to IIS, the responsibility for strict confidentiality, privacy and security remain fundamental to IIS operations.[31] An IIS needs to ensure that electronic immunization information is transmitted to other entities and stored in a secure manner. The HIPAA Security Rule represents security best practice, covering administrative, physical, technical safeguards for electronic data, addressing for example, data backup, disaster recovery, emergency operations, and transmission of information. As such, they ensure

compliance with IIS Functional Standards for implementation by CDC-funded Immunization programs. The American Registry Association (AIRA) has issued a resource document regarding compliance with HIPAA security standards.[32]

The U.S. Department of Human Services, Office for Civil Rights, has issued guidance about the responsibilities of a HIPAA covered entity for electronic health information exchange in a networked environment.[33] An HIE is generally not a HIPAA covered entity. The functions an HIE typically performs do not make it a health plan, health care clearinghouse, or covered health care provider. However, an HIE that performs certain functions or activities on behalf of, or provides certain services to, a covered entity which require access to PHI would be considered a business associate under the Privacy Rule. This means that covered entities that use HIEs to transmit immunization information must enter into business associate agreements with those HIEs.[34] HHS provides guidance on considerations in developing and implementing a business associate agreement with an HIE.

An HIE may manage the exchange of PHI through a network on behalf of multiple covered entities. The HIPAA Privacy Rule does not prohibit an entity from acting as a business associate of multiple covered entities and performing functions or activities that involve access to protected health information for the collective benefit of the covered entities. In addition, the Privacy Rule would not require separate business associate agreements between each of the covered entities and the business associate. Rather, the Privacy Rule would permit the covered entities participating in a networked environment and the HIE to operate under a single business associate agreement that was executed by all participating covered entities and the common business associate.[35]

Family Educational Privacy Rights Act (FERPA)

Many jurisdictions have school and child care immunization laws that require all students enrolling in school to show evidence that they have received certain immunizations or to properly document exemptions. Schools are responsible for assuring that their students are in compliance with the immunization law.

Immunization Programs across the country have implemented school modules in the IIS to provide schools with an official copy of a student's immunization history for maintaining records, as needed for compliance with school immunization laws. These modules are saving schools time by allowing them to have access to multiple students' records in one location, and to quickly identify students missing immunizations, in case of a disease outbreak at a school or in the community.

The level of access varies jurisdiction to jurisdiction. Schools use IIS to look up and print immunization records of students. In addition to using the IIS to view students' immunization records, some schools enter immunization data into the IIS to the extent permitted by FERPA.

FERPA applies to information about students maintained in school records. It prohibits schools from disclosing identifiable information about a student unless his or her parent consents or an exception applies. FERPA does not prohibit schools from accessing information in IIS. Depending on state law, schools may receive immunization data to monitor students' compliance with mandatory student immunization laws. However, FERPA limits information that schools may disclose about students to public health agencies and others, absent the parent's consent.

In the event of a public health or safety emergency, FERPA would allow disclosure of necessary information without a parent's consent.[36] FERPA also allows schools to disclose certain directory information about its students, which includes a student's name, address, telephone number, email address, date and place of birth, dates of attendance, most previous school attended and grade level.[37] This means, absent objection by the parent, public health departments are able to obtain directory information to update their records about children they serve. For example, schools might provide updated addresses for children to immunization programs that send reminders to parents that their child is due for a vaccine. In some states, school personnel may even be provided with access to the IIS to directly update contact information for students because FERPA allows schools to provide electronic directory information.[38]

If a school provides individually identifiable information to the IIS, with the exception of directory information,[39] the IIS is limited in re-disclosure of this information.[40] An IIS may not share most school-entered information with providers, health plans, or others that have access to the IIS. Immunization Information Systems may filter school-entered information from medical providers. For example, if a school adds a varicella to a student's immunization record in the IIS, the physician managing this student's health care would not be allowed to see the varicella dose added by the school. The provider would have to receive this information from the parent or from the previous provider. Similarly, absent consent, an IIS cannot provide most school-entered information to another IIS.

G. Legal Issues related to Data Sharing Agreements (DSA)

Some laws may require entities that exchange health information to enter into data sharing, data exchange, or similar agreements. For example, Michigan law authorizes MDCH to transmit registry information "by written agreement."[41] Even if the law does not explicitly require an agreement, jurisdictions that intend to exchange immunization information should develop an

agreement. Through an agreement, a public health agency sets out its legal authority (both to enter into an agreement and exchange information), specifies terms for sharing, and provides for monitoring and accountability for compliance with these terms. On its website, the Joint Public Health Informatics Taskforce has posted practical guidance for public health agencies that are entering into an inter-jurisdictional, health department to health department, data exchange relationship.[42]

The following data sharing agreements and templates for exchanging immunization information are available on the American Immunization Registry Association website:[43]

- Inter-State Agreement Between State of Washington, Department of Health And State of Oregon, Department of Human Services, State Public Health
- Data Exchange Agreement between The New York State Department of Health and The New York City, New Jersey and Pennsylvania Departments of Health for Immunization Information System Data Exchange
- Inter-Organizational Agreement Template prepared by The Health Information Security and Privacy Collaboration
- Interstate Data Sharing Agreement Template
- Sample Inter-Agency Data-Sharing Agreement

Appendix C describes components that states should consider for inclusion in an immunization data sharing agreement.

H. Four-step Approach to Review Law for IIS Information Sharing

In working with their attorneys, immunization managers may find the following four-step approach to be helpful in addressing legal issues for the wide range of structures for cross-jurisdictional sharing of immunization information.

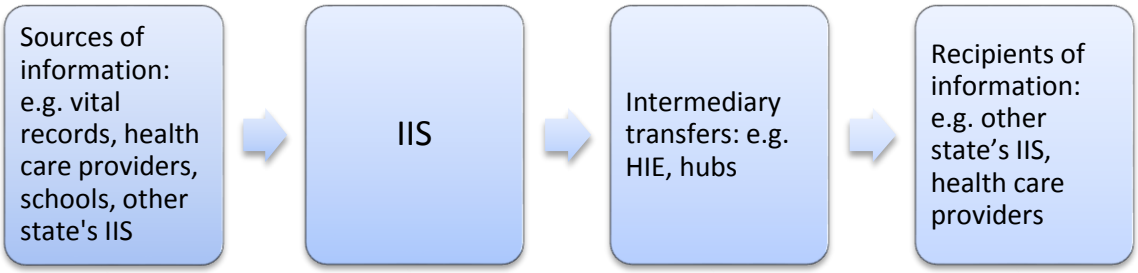
1. **Establish facts.** Factual information about the data to be shared and the circumstances for sharing is needed to evaluate proposed data sharing. Appendix D is a checklist of factual information needed for public health agencies to address proposed data collection, access, and sharing in general. In particular, for access to and sharing of IIS information, answers to the following questions should be considered.

Practice Pointer

To determine authority to share immunization information:

1. **Establish facts**
    a. **Data**
    b. **Participants**
    c. **Flow**
2. **Identify law**
3. **Apply law**
4. **Establish & document terms for sharing**

a. Data: What information do you want to share? What are the data elements? What is the source of the data? What restrictions or conditions apply to data elements?
b. Participants: Who provides and will access or obtain this data. Public health agencies? Health care providers? Schools?
c. Flow – Data movement may be straight-forward, as described in scenarios 1-3 above (Provider or IIS-IIS exchange). It may be complex, as described in scenarios 4-5, with multiple transfer points through a health information exchange or other exchange structure. Every transfer point for data is a decision point with regard to law. To facilitate analysis, immunization managers may want to map the flow of data for their attorneys. Information may flow in one direction (as illustrated below) or bi-directionally (for example, IIS←→IIS or IIS←→health care provider, via HIE).



2. **Identify applicable law.** Providing factual information to your attorney assists him or her to identify law that might apply. As discussed above, applicable laws include those that establish public health's legal authority to share immunization data, privacy and confidentiality laws, and laws that apply to health information or health information exchanges.
3. **Apply law.** Review law of both sending and receiving state. What sharing does law authorize with regard to data elements and parties? What are the prerequisites, conditions, or limitations?
    a. Review law that applies to IIS
        i. Does it authorize cross-jurisdictional sharing?
        ii. Are there any restrictions?
        iii. Who are permitted users?
        iv. If parent or individual consent is required for inclusion of information in IIS, does consent permit proposed sharing?
    b. Review law that applies to each source of information
        i. Are there restrictions on re-disclosure of information?

c. Review law that applies to conduit of information (i.e. intermediary that transfers information to/from IIS)
    i. Are there any legal terms or restrictions?
4. **Establish and document terms for sharing.** These terms are set out in a written data sharing agreement or similar document.

VII. Recommendations

For nationwide cross-jurisdictional immunization information exchange, all IIS must have authority to share immunization information with other jurisdictions. Each jurisdiction should review its law with legal counsel to determine whether state law authorizes immunization information exchange under each of the five scenarios above. For example:

- Access to individual immunization information by providers from one state through the other state's IIS.
- Batch File electronic exchange (from IIS to IIS) of immunization information on any immunization record that has the city or state field that matches the jurisdiction in which the cross-jurisdiction data sharing agreement is implemented. Example: Once a month Michigan could extract data from their IIS on all patients with Wisconsin addresses, and send the immunization data in a secure batch file format to Wisconsin.

Prerequisites, conditions and limitations should be identified. Authority may be clarified by a state Attorney General Opinion. If current authority does not exist or is too limited to accomplish goals, states will need to develop a plan to obtain needed authority, which could include development and adoption of statutes, regulations, or policies.

States should consider passing legislation that ensures the timely, secure interstate exchange of immunization information. Ideally, states would pursue legislation that promotes uniformity among states. To assist states that would like to begin sharing immunization information across state lines, Every Child By Two partnered with the Department of Health Policy at The George Washington University School of Public Health and Health Services to create the Model Interstate Immunization Information Sharing Statute.[44] The model statute addresses the seven elements that are necessary for inclusion in a statute intended to promote exchange of immunization data for personal and public health purposes while protecting the confidentiality of personal information. The model statute will not alter the state's current notification and opt out requirements. This model statute was developed in 2005, so it should be reviewed to

ensure that it addresses current concerns. If a state has rulemaking authority to provide for cross-jurisdictional sharing, a model statute might be adapted into a rule.

Variations in state laws present challenges to cross-jurisdictional sharing of immunization information system data. Ideally, a federal law that provides for a national IIS could facilitate nationwide exchange. However, this may be no more obtainable today than it was in 1993 when Congress failed to pass provisions that would have created a national immunization registry as part of the Child Health Immunization Act. Alternatives to a national IIS should be explored, such as federal promotion and support of using health information exchange to facilitate immunization information sharing.

While a national IIS might not be feasible, the federal government might use funding as an incentive to create state-based IIS that promote and facilitate cross-jurisdictional data sharing. Technological, as well as legal, solutions are needed to support immunization information exchange. Federal funding could provide some of the resources necessary to meet the challenges of developing cross–jurisdictional immunization information exchange.

In addition to variation of laws among states, variations in data-related laws within a state can create barriers to cross-jurisdictional exchange. Multiple laws within a state may impact sharing of immunization information. These may include laws governing data that populates the IIS, such as laws regarding vital records, information provided by schools, and using health information exchange to transmit health information. States need to review and work to harmonize any laws that interfere with the flow of immunization information. For example, a state's HIE consent law should be compared to its IIS consent law to ensure that they do not work at cross-purposes.

To support IIS interstate data sharing, development of a model interstate data sharing agreement should be explored. The North American Association of Central Canter Registries (NAACCR) has developed a model National Interstate Data Exchange Agreement as an efficient way for states to exchange cancer incidence data.[45] This single agreement will take the place of multiple interstate data exchange agreements. NAACCR has posted a matrix that has a column for each registry with date signed, restrictions, permissions, and contact person email. So far, 23 state registries have signed.

Another option – recommended to the National Vaccine Advisory Committee by a group of stakeholders– is to explore the feasibility of using the National Association for Public Health Statistics and Information Systems (NAPHSIS) interstate transfer standard agreement model for IIS interstate data exchange for both IIS and individual providers.[46] NAPHSIS administers an inter-jurisdictional exchange agreement (IJE) whereby participating jurisdictions agree to

electronically exchange vital event information through the State Territorial Exchange of Vital Events (STEVE) system.[47] When preparing an IJE Agreement, each jurisdiction specifies restrictions and allowances to use of their vital records by other jurisdictions in accordance with their own legal and policy situations. Receiving jurisdictions agree to abide by the restrictions of sending jurisdictions when using received records.

References

[1] Development of Community- and State-Based immunization Registries, Report of the National Vaccine Advisory Committee (NVAC) (January 12, 1999). Available at http://archive.hhs.gov/nvpo/report071100.pdf. Accessed July 30, 2014.

[2] Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act, Pub. L. 111-5, 42 U.S.C. 300jj *et seq.*; 17901 *et seq*.

[3] American Recovery and Reinvestment Tax Act of 2009, Pub. L. 111-5, 123 Stat. 306.

[4] Proposed Immunization Information Systems (IIS) Strategic Plan v1.3 November 30, 2014. Center for Disease Control, National Center for Immunization and Respiratory Diseases.

[5] CDC, Immunization Information System (IIS) Functional Standards. Available at http://www.cdc.gov/vaccines/programs/iis/func-stds.html. Accessed July 30, 2014.

[6] Section 317(j) of the Public Health Service Act (42 U.S.C. 247b(j)).

[7] CDC, Immunization Information Systems, Contacts for Immunization Records. Available at http://www.cdc.gov/vaccines/programs/iis/contacts-locate-records.html. Accessed July 30, 2014. Martin DW, Lowery NE, Brand B, Gold R, Horlick G. Immunization Information Systems: A Decade of Progress in Law and Policy. J Public Health Management Practice, 2013, 00(00), 1-8. Available at http://www.immregistries.org/resources/Immunization_Information_Systems___A_Decade_Laws_998321.pdf. Accessed July 30, 2014.

[8] New Hampshire Department of Health and Human Services, Meaningful Use in the Division of Public Health Services. Available at http://www.dhhs.nh.gov/dphs/bphsi/meaningful-use.htm. Accessed July 30, 2014.

[9] Martin DW, Lowery E, Brand B, Gold, R, Horlick G. Immunization Information Systems: Decade of Progress in Law and Policy. J Public Health Management Practice, 2013 00(00), 1-8Available at http://journals.lww.com/jphmp/Citation/publishahead/Immunization_Information_Systems___A_Decade_of.99832.aspx. Accessed July 30, 2014.

[10] IISARs are available on the CDC's website at http://www2a.cdc.gov/nip/registry/IISAR/IISAR_QUERY.asp. Accessed July 30, 2014.

[11] HRSA, Health Information Technology, What is Health Information Exchange? Available at http://www.hrsa.gov/healthit/toolbox/RuralHealthITtoolbox/Collaboration/whatishie.html. Accessed November 20, 2014.

[12] Fairchild, AL, Gable, L, Gostin, LO, Bayer, R, Sweeney, P, Janssen, RS. Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information. Public Health Rep. 2007; 122(Suppl 1): 7–15. Available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1804110/. Full text of the Comprehensive Child Immunization Act of 1993 joint hearing before the Committee on Labor and Human Resources, United States Senate, and the Subcommittee on Health and the Environment of the Committee on Energy and Commerce, House of Representatives, April 21, 1993, is available at https://archive.org/stream/comprehensivechi00unit/comprehensivechi00unit_djvu.txt. Both URLs accessed July 30, 2014.

[13] Arzt N, HLN Consulting LLC, Towards a National IIS Strategy: Options for Developing a National Immunization Information System Architecture. May 2014 (v4). Available at https://www.hln.com/assets/pdf/HLN-National-IIS-Architecture-White-Paper.pdf. Accessed July 30, 2014.

[14] Information about the pilot project is available on ONC's website at http://www.healthit.gov/providers-professionals/health-information-exchange/nationwide-hie-strategy. Accessed August 6, 2014.

[15] Daniel J, ONC Immunization Registry Data Exchange Pilot Program, SNAPSHOTS, IMMUNIZATION REGISTRY NEWS *from* AMERICAN IMMUNIZATION REGISTRY ASSOCIATION (AIRA), January 2014. Available at file:///Users/denichry/Downloads/SnapShots%20(Jan-14).pdf. Accessed July 30, 2014.

[16] HHS, The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf. Accessed July 30, 2014.

[17] Connecticut and Rhode Island do not collect information on adults. Currently, New Hampshire does not operate an IIS.

[18] ORS §§ 433.090(5), 433.092, 433.098.

[19] Oregon Admin Rules, 333-049-0040.

[20] MCL 333.9207, MCL 333.9227.

[21] Michigan Admin Code, R 325.168.

[22] Boom JA, Dragsbaek AC, Nelson CS. The success of an immunization information system in the wake of Hurricane Katrina. Pediatrics 01/2007; 119(6):1212-7.

[23] NRS 439.538; NRS 439.591.

[24] M.G.L.A. 118I § 13.

[25] 45 C.F.R. Parts 160 and 164.

[26] Pub. L. 104-191, 42 U.S.C. §300gg *et seq*.

[27] Pub. L. 93-380, 20 U.S.C. §1232g, implemented by 34 C.F.R. Part 99.

[28] MMWR, HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services, April 11, 2003 at http://www.cdc.gov/privacyrule/guidance/PRmmwrguidance.pdf. 45 CFR 164 CFR §§164.506, 164.512(a), 164.512(b). Accessed July 30, 2014.

[29] Martin DW, Lowery E, Brand B, Gold, R, Horlick G. Immunization Information Systems: Decade of Progress in Law and Policy. J Public Health Management Practice, 2013 00(00), 1-8. Available at http://www.immregistries.org/resources/Immunization_Information_Systems___A_Decade_Laws_998321.pdf. Accessed July 30, 2014.

[30] 45 CFR §§160.202, 160.203.

[31] Immunization Information System (IIS) Functional Standards, CDC (2013-2017). Available at http://www.cdc.gov/vaccines/programs/iis/func-stds.html. Accessed July 30, 2014.

[32] HIPAA Security Rules – Guidance for Immunization Registries, Version 1, October 2004, American Immunization Registry Association; Prepared by AIRA Technical Committee, HIPAA Security Rule Task Group. Available at http://www.immregistries.org/resources/HIPAA_v2.pdf. Accessed July 30, 2014.

[33] The HIPAA Privacy Rule and Electronic Health Information in a Networked Environment. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf. Accessed July 30, 2014.

[34] 45 CFR §164.504.

[35] The HIPAA Privacy Rule and Electronic Health Information in a Networked Environment. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf. Accessed July 30, 2014.

[36] 34 C.F.R. §§99.31(a)(11), 99.36. This exception is narrower than HIPAA's "public health" exception to authorization. If it is determined that there is an articulable and significant threat to the health or safety of a student or other individuals, a school may disclose information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. For example, during a measles outbreak, FERPA would permit school officials to disclose to public health authorities their students' immunization records to determine whether or not they are vaccinated for measles. However, the FERPA "health and safety exemption" would not allow schools to provide routine information regarding immunization to an IIS without the parent's consent. See Dept of Education guidance at http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-disaster-guidance.pdf. Accessed July 30, 2014.

[37] 34 C.F.R. §§99.31(a)(11), 99.37.

[38] Revised FERPA Regulations May Impact Health Departments Access to Children's Contact Information, Network for Public Health Law, posted on May 25, 2012, by Denise Chrysler. Available at https://www.networkforphl.org/the_network_blog/2012/05/25/106/revised_ferpa_regulations_may_impact_health_departments_access_to_childrens_contact_information. Accessed July 30, 2014.

[39] 34 C.F.R. §99.33(c).

[40] 34 C.F.R. §99.33(a).

[41] Michigan Admin Code, R 325.168.

[42] Joint Public Health Informatics Taskforce, Inter-Jurisdictional Health Information Exchange, Guidance for Public Health Agencies. Available at http://www.phii.org/resources/view/5909/Inter-Jurisdictional%20Health%20Information%20Exchange. Accessed July 30, 2014.

[43] American Immunization Registry Association, Data Sharing Agreements. Available at http://www.immregistries.org/resources/data/data-sharing-agreements. Accessed November 20, 2014.

[44] Every Child by Two, Print Materials, Model Interstate Data Sharing Law. Available at http://www.ecbt.org/index.php/strategies_and_resources/article/print_materials. Accessed July 30, 2014.

[45] National Interstate Data Exchange Agreement. Available at http://www.naaccr.org/StandardsandRegistryOperations/DataExchangeAgreement.aspx. Accessed July 30, 2014.

[46] NVAC, Enhancing Participation in Immunization Information Systems (IIS): Recommendations to the National Vaccine Advisory Committee. Available at http://www.hhs.gov/nvpo/nvac/iisrecommendationssep08.html. Accessed July 30, 2014.

[47] NAPHSIS, Inter-Jurisdictional Exchange of Vital Records. Available at http://www.naphsis.org/Pages/InterJurisdictionalExchangeVitalRecords.aspx. Accessed July 30, 2014.

Appendix A: IIS to IIS Exchange of Immunization Information

(This information is based on self-reported data from the grantee IISARs for 2011)

Jurisdiction	**Exchanges information with other IIS**	**Specific jurisdictions with which state IIS exchanges information**	**Exchange capabilities** Flat file exchange HL7 unidirectional - Real time, Batch HL7 bidirectional - Real time, Batch
Alabama	No		
Alaska	No		
Arizona	Yes	Washington	HL7 bidirectional - Real time
Arkansas	No		
California	No		
Colorado	No		
Connecticut	No response		
Delaware	No		
District of Columbia	No		
Florida	No		
Georgia	No		
Hawaii	No		
Idaho	No		
Illinois	No		
Indiana	Yes	Louisiana	HL7 bidirectional - Real time
Iowa	No		
Kansas	No		
Kentucky	No		
Louisiana	Yes	Mississippi; Houston	Flat file; HL7 bidirectional - Real time
Maine	No		
Maryland	No		
Massachusetts	No		
Michigan	No		
Minnesota	Yes	Wisconsin	Flat file
Mississippi	Yes	Louisiana	HL7 bidirectional - Real time
Missouri	No		
Montana	No		
Nebraska	No		
Nevada	No		
New Jersey	No		
New Mexico	No		
New York City	Yes	New York State	Flat file
New York State	Yes	New York City	Flat file
North Carolina	No		
North Dakota	No		
Ohio	No		
Oklahoma	No		
Oregon	Yes	Washington	Flat file
Pennsylvania	No		
Philadelphia	Yes	Pennsylvania state	Flat file

Jurisdiction	Exchanges information with other IIS	Specific jurisdictions with which state IIS exchanges information	Exchange capabilities Flat file exchange HL7 unidirectional - Real time, Batch HL7 bidirectional - Real time, Batch
Rhode Island	No		
San Antonio	No		
South Carolina	No		
South Dakota	No		
Tennessee	No		
Texas	No		
Utah	No		
Vermont	No		
Virginia	No		
Washington	Yes	Arizona; Idaho; Louisiana	Flat file; HL7 bidirectional - Real time
West Virginia	No		
Wisconsin	Yes	Minnesota	Flat file
Wyoming	No		

Source: IISAR

Question 60

Does your IIS exchange data grantee to grantee? ☐ Yes☐ No If yes, which states/cities _____.

Question 61

If yes to 60, indicate how you exchange data below (check all that apply).

__Flat file exchange

__HL7 unidirectional ☐ Real time ☐ Batch

__HL7 bidirectional ☐ Real time ☐ Batch

Appendix B: Authority By Jurisdiction To Operate An IIS

Jurisdiction	Age Group	Authority to operate an IIS (children's registry)	Type of consent from a Parent	Type of consent from an Adult
Alabama	Life Long	Statute/regulation that is specific to sharing immunization information	Implicit consent with Opt Out	Implicit consent with Opt Out
Alaska	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Arizona	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Explicit consent, written
Arkansas	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Explicit consent, written or verbal
California	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Colorado	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Connecticut	Children only	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Other
Delaware	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Mandatory, with no right to opt out
District of Columbia	Life Long	Statute/regulation that is specific to sharing immunization information	Mandatory, with no right to opt out	Other
Florida	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Georgia	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Hawaii	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Idaho	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Illinois	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Indiana	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Iowa	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Kansas	Life Long	General public health statute/regulation	Explicit consent, written	Explicit consent, written
Kentucky	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Louisiana	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Maine	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Maryland	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out

Jurisdiction	Age Group	Authority to operate an IIS (children's registry)	Type of consent from a Parent	Type of consent from an Adult
Massachusetts	Life Long	Specific IIS enabling statute/regulation	Mandatory, with right to opt out	Mandatory, with opt out
Michigan	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Minnesota	Life Long	Statute/regulation that is specific to sharing immunization information	Implicit consent with Opt Out	Implicit consent with Opt Out
Mississippi	Life Long	Statute/regulation that is specific to sharing immunization information	Mandatory, with no right to opt out	Mandatory, with no right to opt out
Missouri	Life Long	General public health statute/regulation	Mandatory, with no right to opt out	Mandatory, with no right to opt out
Montana	Life Long	General public health statute/regulation	Explicit consent, written or verbal	Explicit consent, written or verbal
Nebraska	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Nevada	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
New Jersey	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Explicit consent, written
New Mexico	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
New York City	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Explicit consent, written
New York State	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Explicit consent, written or verbal
North Carolina	Life Long	Statute/regulation that is specific to sharing immunization information	Mandatory, with no right to opt out	Mandatory, with no right to opt out
North Dakota	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Implicit consent with Opt Out
Ohio	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Oklahoma	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Oregon	Life Long	Specific IIS enabling statute/regulation	Mandatory, with right to opt out	Implicit consent with Opt Out
Pennsylvania	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Philadelphia	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Rhode Island	Children only	Specific IIS enabling statute/regulation	Other, Reporting is mandatory in RI with no consent	Other

Jurisdiction	Age Group	Authority to operate an IIS (children's registry)	Type of consent from a Parent	Type of consent from an Adult
			needed. However, parents may opt out of having their information shared but it still has to be reported.	
San Antonio	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
South Carolina	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Mandatory, with no right to opt out
South Dakota	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Tennessee	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Texas	Life Long	Statute/regulation that is specific to sharing immunization information	Explicit consent, written	Explicit consent, written
Utah	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Vermont	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Mandatory, with no right to opt out
Virginia	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Washington	Life Long	Statute/regulation allowing sharing of health care information (but is not specific to immunizations)	Implicit consent with Opt Out	Implicit consent with Opt Out
West Virginia	Life Long	Specific IIS enabling statute/regulation	Mandatory, with no right to opt out	Mandatory, with no right to opt out
Wisconsin	Life Long	General public health statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out
Wyoming	Life Long	Specific IIS enabling statute/regulation	Implicit consent with Opt Out	Implicit consent with Opt Out

Source: Data gathering and analysis conducted by the Public Health Informatics Institute Decatur, GA, under the cooperative agreement number HM08080502CONT12 from the Center for Disease Control and Prevention. CDC has posted these results on its website at http://www2a.cdc.gov/vaccines/iis/iissurvey/legislation-survey.asp. Accessed July 30, 2014. CDC warns that it has not finalized this data, so it is subject to change.

Appendix C: Components Of An Immunization Data Sharing Agreement

Sample provisions and legal/policy considerations

The following section contains suggested provisions and issues for consideration when contemplating immunization information Data Sharing Agreements (DSA). This document is not intended to give legal advice. Leadership and legal counsel in each jurisdiction must be consulted prior to developing a DSA.

Parties and signatories

In general, the public health department or immunization section that has responsibility for the IIS will be the named party to the DSA, not the IIS. Laws and policies in each jurisdiction identify positions of those who are authorized to execute agreements on behalf of each state agency.

Rationale, purpose, and public benefit

The first few paragraphs of the DSA should state the general public health purpose of the agreement and the statement of the problem addressed by the DSA. In most instances, the rationale for the DSA will be to allow the IIS to exchange information relating to residents of one jurisdiction who receive health care in another jurisdiction, or who have moved to another jurisdiction. The mutual goals and benefits for each party are to allow protection of public health through delivery of medical care and to control vaccine preventable diseases.

Confidentiality

Include a statement of the importance of maintaining the confidentiality of the information exchanged with citations to applicable laws.

Statement of no monetary exchange

State that each jurisdiction will provide its own personnel, equipment, material and services to comply with the agreement and that there is no exchange of funds.

Authorities

Identify the statutory/regulatory reference of authority to operate an IIS, to provide access (disclose) to the other parties (e.g., a different State's IIS, HIE or health care provider), and to enter into the DSA.

Application of HIPAA

State whether or not each party to the agreement is subject to HIPAA.

Period of agreement

State the beginning and end dates of the DSA. Some jurisdictions do not allow agreements to become effective until the date executed by the last of all required signatures. Other jurisdictions will allow agreements to become effective on a stated date. An "as of" effective date is usually more clear. There should be stated review dates (e.g., every two or three years) to keep the DSA provisions up to date.

Information to be exchanged

Document exact data fields that will be exchanged, their format, frequency of sharing data, and the method of secure transport. This information should be included in an Appendix that can be modified by the parties, if necessary. Data fields, format and transport should comply with published standards, including the CDC HL7 Implementation Guide. http://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html

The DSA can state that the schedule of the data exchange can be at a time mutually agreed upon by the parties. The DSA can state that there is no guarantee that an IIS will be operational and/or be capable of sending data on an uninterrupted basis (e.g., there is no guarantee that there will be no scheduled or unscheduled down time).

Ownership

The term "ownership" can include a number of related, but independent concepts. Use of the term "ownership" alone, without definition, is ambiguous and subject to misunderstanding. To be clear, each of the concepts should be explicitly addressed in the DSA.

- Incorporation of data. State that the data received is permitted to be incorporated into the receiving IIS.
- Use and disclosure of data. See "Use and disclosure of information" below.
- Disposition of data. See "Disposal of information" below.

Warranties

State that no party guarantees the accuracy or completeness of the data exchanged under the DSA. The parties may go on to state that each party will use its best efforts to ensure the accuracy and completeness of the data exchanged under the DSA. Any affirmative statement such as "best efforts to ensure" may be limited by other provisions of the DSA. See "Limitation of liability" below.

- State that each party will use its own independent professional judgment as to whether or not to incorporate, use and disclose any data exchanged under the DSA.
- State that no IIS warrants that the data delivery will be uninterrupted (i.e., that the sending IIS will not be operational without scheduled or unscheduled down time).

Limitation of liability

State that no party is liable for any damages.

State that the parties will not have any recourse against each other and each waives claims of any kind for use or misuse of information exchanged under the DSA.

Use and disclosure of information exchanged under the DSA

State the permitted uses and disclosures of information exchanged under the DSA. Different models of how the laws and policies of each jurisdiction might apply to shared immunization information are:

- The laws and policies applicable to the receiving party solely determine how the information can be used and disclosed.

- The information shared remains subject to the laws and policies of the sending IIS. Each party must be capable of meeting the requirements of the more restrictive jurisdiction.

Monitoring and notice of breach

State that each IIS will give notice to the other party of any breach or attempted breach of confidentiality.

Disposal of information

State how the information will be identified after sharing, if required, and the method of disposal of the information (e.g., after the purposes of a project are accomplished). If immunization data is used for public health research purposes, a method of disposal should be included in the DSA.

Incorporation of laws and policies by reference (including IIS Confidentiality Policy and Security Policy)

A DSA should incorporate state and federal laws by reference, stating that the parties will comply with all federal and applicable state laws. Incorporation of all applicable laws puts the burden of determining the applicable laws and their impact on each party, which could be burdensome. As noted under "Use and disclosure of data" above, laws differ with respect to permissive disclosures of IIS information, and are subject to interpretation. Laws and policies may also change during the course of a DSA. A DSA would be clearer if it detailed the impact of laws on shared information. If applicable laws and policies are incorporated by reference, a DSA can require each party to notify each party to the DSA of any change in its laws and policies and the effect on the DSA.

Security and Confidentiality Policies

Each party should agree to provide notice to other participants if its Security or Confidentiality Policies are amended.

General Provisions

How to amend - Amendments to a Data Sharing Agreement must be made in writing and signed by authorized representatives of both parties.

Termination - Any party may terminate a DSA if the other party is in default of any condition of the DSA and such default has not been remedied within 30 days after the date of written notice.

*Termination for caus*e – The DSA is terminated if one party breaches the DSA or if it conflicts with applicable laws. A party may terminate a DSA at any time if it is determined that a party has failed to comply with the conditions of the DSA.

Governing laws - The DSA can be silent on governing law.

Assignment – There should be no waiver of any requirement of the DSA without written consent. The parties that share immunization data with each other shall not assign or transfer the DSA or any part of the agreement without the prior review and written consent of the other parties.

Waiver - Failure to give notice of breach of a provision does not waive that provision. Example: If organization A breaches a component of the DSA between organization A and B, and organization B fails to notify organization A of its breach, this does not constitute a wavier of that breach by organization B.

Severability - if one provision of the DSA is not enforceable it does not affect other provisions.

Notices - Provide the names and contact information of individuals to whom notice should be given. Notices or communications to or between DSA participants may be delivered (a) by email notification; (b) by deposit in the U.S. mail when mailed by first class mail; (c) if sent by established courier service; or (d) when received by a participant, if personally delivered.

Integration - The DSA specifies all the information for sharing data between the parties. Any representation, promise, or condition, whether oral or written, not incorporated in the DSA is not binding.

Force Majeure - There is no breach of the DSA if a force of nature prevents compliance. There is no breach of the DSA in the event of a disruption, delay or inability to complete the requirements of the DSA due to natural disasters, acts of terror or other similar events

Counterparts - If permitted by law, multiple copies of the DSA can be signed.

Authority to Sign – This states the parties are authorized to sign.

Third Party Beneficiary - No one other than the parties to the DSA have any rights under the DSA.

Appendix D

The Network for Public Health Law

Ideas. Experience. Practical answers.

Checklist of Factual Information Needed for Public Health Agencies to Address Proposed Data Collection, Access and Sharing

Public health attorneys and privacy officers provide advice to public health agencies on an array of questions about collecting, accessing, and sharing information. Questions may involve oral, written or electronic data. Responses must consider whether a public health agency has the legal authority to collect, access, or share information, and if so, what are the conditions and limitations for data sharing. In addition to legal considerations, policy and ethical concerns may be relevant. In some situations - for example, urgent threats of communicable disease – the public health agency might face competing interests of protecting individual privacy and protecting the public's health. Certain factual information about the data to be shared and the circumstances and conditions for sharing is needed to evaluate proposed data sharing. The checklist below is intended to assist public health practitioners in providing relevant factual information to resolve questions about proposed data collection, access and sharing.

What?

What information do you want to obtain or share? Identify data elements.

Why?

For what purpose is this information needed? Clearly articulate the public health purpose.

How Much?

Will de-identified information or a limited data set (that includes demographics but not personal information) serve the purpose?

From whom?

What are the sources for the information? (e.g. health care providers, schools, other business, and individuals that provided/will provide the information to public health).

Under what terms or conditions, if any, was this information provided to you?

January 2014

With whom?
Who will have access to this information?

Conditions?
Acceptable uses and linkages of the information?

How? Where?
How will the information be transferred/shared/stored?

Protections?
What privacy and security measures are in place to protect information during transfer, storage, use and disposal?

And then what?
Retention, reuse, further sharing, disposal of the data?

Assurance?
Audits or other mechanisms to monitor proper receipt, storage, access and use?

Accountability?
What are the terms of data use and means to enforce for violations?

Supporters

The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation with direction and technical assistance by the Public Health Law Center at William Mitchell College of Law.

This document was developed by Denise Chrysler, J.D., Director, at the Network for Public Health Law – Mid-States Region. The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.