The Network for Public Health Law

Data Across Sectors for Health

Pathways to Yes

A legal framework for achieving data sharing for health, well-being, and equity

Contents

Introduction 1

Step 1: Review Relationships 3

Step 2: Develop a Use Case 5

Step 3: Create a Data Flow Map. 10

Step 4: Conduct the Legal Analysis 11

Step 5: Establish and Document Agreements for Sharing 15

Conclusion 17

References 18

Glossary 19

Appendix 20

I. Fall Prevention Case Study 20

II. Housing and Health Case Study 24

III. Incarcerated Individuals and Behavioral Health Case Study 27

IV. Medical-Legal Partnership Case Study 31

V. Opioid Misuse Prevention Case Study 34

This document was developed by The Network for Public Health Law (NPHL) and Data Across Sectors for Health (DASH). Primary NPHL authors were Jennifer Bernstein, Deputy Director, and Denise Chrysler, Regional Director, from The Network for Public Health Law – Mid-States Region, and the primary DASH author was Peter Eckart. Contributing NPHL authors were Sallie Milam, Colleen Healy Boufides, Jill Krueger, and Chris Alibrandi O'Connor.

Document Key

CASE STUDIES

This publication outlines five main and several smaller steps to help people navigate the legal complexities of data sharing. Each step described in this document will correspond to a specific segment within each of the five case studies at the end of this publication. Using the in-document links, you can navigate between the descriptions of the steps and the relevant examples in the case studies.

TYPES OF LINKS

In-document link External/web link

Introduction

The legal issues relevant to data sharing, particularly cross-sector data sharing, are not necessarily barriers, but they are often perceived to be.[i] That's why one frustrated practitioner, staring down one legal roadblock after another, described their attempts to share data among community health organizations as "wandering in the Land of No."

But it doesn't have to be that way: if practitioners possess key knowledge of relevant legal frameworks, including state and federal laws, it can go a long way towards advancing collective community health goals, particularly health equity.

Easier said than done, maybe. Being legally compliant can be daunting even for those with legal training. The large volume of potentially applicable laws can be overwhelming and conducting a comprehensive analysis of all proposed data types and sources requires significant support. Yet, these aren't impossible tasks.

That's why we've put together this resource. This report is meant to help you navigate the legal parameters of data sharing, and encourage you to collect, integrate, and use multi-sector data to improve individual and community health, well-being, and equity.

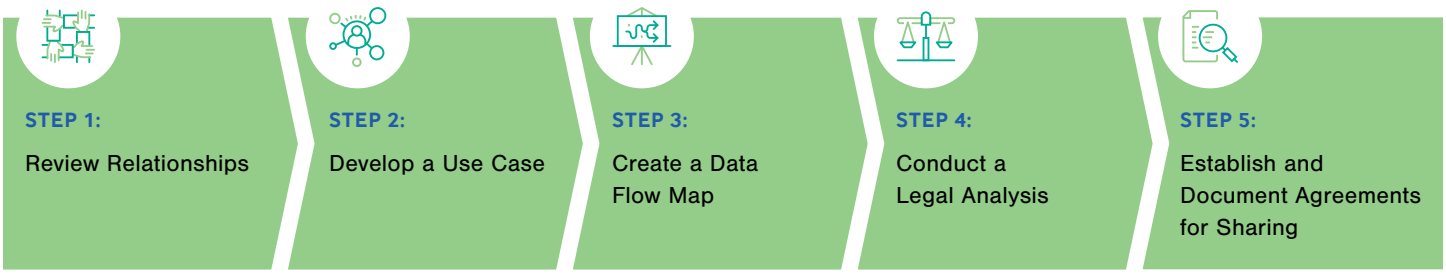
By way of background, there is a growing body of literature demonstrating how a broad range of physical, environmental, and social factors – 'social determinants of health' – affect the health and well-being of individuals and communities. It follows that acquiring timely, reliable, granular data from many different sources can help us develop effective strategies to improve health outcomes and support health equity.

The sources of data tend to vary greatly. They might include local, state, and national surveys, public health surveillance and program data, clinical data, environmental data, community partner data, administrative data, and much more.

All this points to the increasing importance of sharing data across different sectors. But sharing data entails more than meets the eye. The work includes wading through many different organizations, systems, data types, and laws. In fact, the data collected and shared often includes personally identifiable health information, which is often protected by state and federal laws that vary widely across jurisdictions.

Our goal for this tool is to help you overcome those barriers and to get you from the "Land of No" onto the "Pathways to Yes."

Structure



Sharing data legally, ethically, and meaningfully means wading through many different organizations, systems, data types, and laws. This report outlines a five-step process to help you analyze the legal complexities of data sharing.

We illustrate each step with case studies based on real-world projects. The projects had been carried out by member organizations of the *All In: Data for Community Health* network. *All In* is a nationwide network of data-sharing initiatives where member organizations actively learn from one another. They collectively build the evidence base for a data system that can improve the health and well-being of communities while centering equity.

Audience

This report is for agencies and organizations that wish to engage in systematic, routine exchanges of information for the purpose of improving individual and population health outcomes.

- Public health, social service, and law enforcement agencies
- Healthcare providers
- Health systems
- Any other community-based organizations

Types of Data

This report addresses various types and sources of data, including protected health information that is regulated under the Health Insurance Portability and Accountability Act (HIPAA). The report is also relevant for other health data – as well as data that could be relevant to social determinants of health and health outcomes, even if the data isn't considered health data traditionally.

Disclosures

The goal of this report is to help you analyze the environment of the kinds of personally identifiable data that can support efforts to improve individual and population health. This report does not delve into the ethics of how data sharing can center equity, which is an area that current law doesn't address well enough. We recommend that you apply our guidance in combination with other resources to center equity in data sharing.

This report is not meant to identify individual laws that may apply within a specific data-sharing context or provide an exhaustive treatise on data-sharing law. The report is not intended to be legal advice from the organizations that created this document, or from the funders of those organizations. Please make sure to always consult your attorney regarding the specifics of your proposed data-sharing project.

STEP 1

Review Relationships

Game theory's stag hunt dilemma describes a problem where everyone must trust that all other participants will do the right thing in pursuit of a collective goal. Sharing data is similar: your project is most likely to succeed only when all participants trust one another.

Internal Partners

Project Champion

The success of your collaboration will largely depend on the relationships within your own organization. In fact, your partners may look for assurance from your leadership team, so it is essential to have buy-in for the project at your organization's highest levels.

This person will be your project champion and will play a vital role. They should be someone in middle or upper management who fiercely supports and advocates for the project. This person should help articulate the benefits of your undertaking to leadership and external stakeholders.

The champion does not have to be the project manager, but they should be involved from its initial conception. They also should be willing to use their authority to offer resources and additional expertise, and ensure the project is sufficiently staffed.

Attorney

Bring your attorney on board during your project's initial phase – and remember that a team member who feels valued will work harder to achieve the project's goals. It's likely that your attorney will have a vested interest in the overall success of your project if they feel like they have ownership in the project and that they fully understand its importance.

Be aware that legal training encourages attorneys to be somewhat risk averse. It is their duty to assist a client in minimizing legal risk, and they therefore may be conservative in their approach. Furthermore, sharing electronic data can itself be a complicated task, requiring some time for your attorney to develop an understanding of the terms and systems involved.

Rather than asking your attorney if a certain type of data sharing is permissible, it may be helpful to present them with the project goals and desired outcomes and demonstrate how you intend to achieve those goals through data sharing. The attorney can identify if there are any laws regulating this exchange. They can also help you sidestep a rigid "yes" or "no" situation, and instead get you on the "Pathway to Yes."

Your Attorney's Role:

- Identify laws that are relevant
- Determine how the law applies to your specific project.
- Offer guidance to ensure legal compliance and minimize risk.
- Provide alternative strategies if legal barriers prevent certain data-sharing pathways.
- Define legal pathways to reach your desired outcome while complying with all legal requirements.

External Partners

You are likely to be more efficient and make quicker progress on your data project when you work with existing partners. This is true even if data sharing had not been the focus of your collaboration in the past. One reason for this has to do with trust. Providing information to another organization means you trust that they will follow all contractual and legal requirements. Having already established that trust saves time and explains why successful data-sharing projects are often built on existing relationships.

This is not to say that you shouldn't expand your reach to new partnerships – especially if they have information that may be crucial to reaching your project goals. Those outside your network may be engaged in similar work or directly connected to the work you are pursuing. In fact, research and analysis provide sound evidence that community engagement in interventions has a positive impact on a range of health outcomes.[ii] That's why we recommend that you engage and establish new partnerships with the community you are trying to support.

As you build data-sharing relationships, consider whether your project will require unidirectional sharing or multi-directional sharing. A unidirectional data sharing collaborative may simply compile relevant data from various sources in order to reach health improvement goals. In a multi-directional data sharing collaborative, partner organizations work to affect the health of your target population. A multi-directional flow of data is generally more legally complex, as will be discussed later.

Assembling the right partners and deciding on a particular problem or opportunity to address usually go hand in hand. The common goals of your organization and its partners naturally drive the focus of activity, and, eventually, the data sharing that supports it. That's why it will be necessary to identify and bring together potential project stakeholders as you put together a specific plan to address the problem or opportunity.

Before getting too far into the process, you and your partners will need to develop consensus on the project's ocus, shared value proposition, health objective and possible interventions. Project leaders need to establish a process to develop agreement among stakeholders. This could consist of formal governance, or simply assigning a designated representative from each stakeholder organization to attend regular project meetings. It is likely that additional stakeholders may be identified later, during the development of the use case. Depending on the new stakeholder's role in the project, you may need to revise the use case and subsequent legal analysis.

STEP 2

Develop a Use Case

Laws relevant to data sharing projects often include a complex system of requirements based on the type of data, its source, and the purpose of data sharing. To help navigate this complexity, law and data professionals have borrowed the concept of 'use cases' from software and systems engineering.[iii]

Earlier, we established the importance of building trust among collaborative partners; a well-defined use case can be just as important to a project's success. Use cases describe the interaction between a system and its users to produce a valuable outcome. More practically, a use case will describe the flow of data within the larger 'system' of your data-sharing initiative. It's also good practice for clarifying and communicating the complex work done by collaborative partners.

The major benefit of a use case is that it can simplify the project development process and legal analysis for your data-sharing projects. It will help you identify and resolve important elements of your project, such as who is involved in the collaboration, the role of key stakeholders, what data is required, and the ways data will be used by the partners who receive it. Finally, it is a necessary process in order to develop a comprehensive legal analysis of your proposed data-sharing activity to identify and resolve any legal issues.

7 Building Blocks of Your Use Case

The order in which you approach each element may change depending on the goals and structure of your project. Once you have completed each component, your attorney can use this information to identify relevant laws and develop a complete analysis to determine the best legal pathways for your proposed data sharing.

1. Health, well-being, and equity: what's your objective?

You must identify the specific health, well-being, and equity objectives your project will address by sharing data. Does your project aim to assess or evaluate the nature and scope of a health problem in your community? In that case, you probably don't have a specific health outcome goal. Is your project aimed at making changes in your community by way of an intervention? If so, then you need to specify your outcome goals. Make sure to state the outcome goals and health, well-being, and equity objectives of your project as specifically as possible.

Your project might begin with an assessment or evaluation phase, then progress to an intervention phase. If you obtain any new information during the evaluation phase, you will need to amend your initial objective to ensure that it is still in line with your community's overall health goals. The outcome goals and health, well-being, and equity objectives should be stated with as much specificity as possible. These details are important to conducting your legal analysis because they help ascertain many of the use case elements we will describe later in this report.

EXAMPLE: Let's say that your goal is to increase the proportion of preschool children aged 5 years and under who receive vision screening in your community. In this case, you will need to identify your community's current baseline and target rates and the desired time frame for achieving the goal. This will help you pinpoint potential data sources and identify the most effective interventions.

Click on an icon to see a case study example:

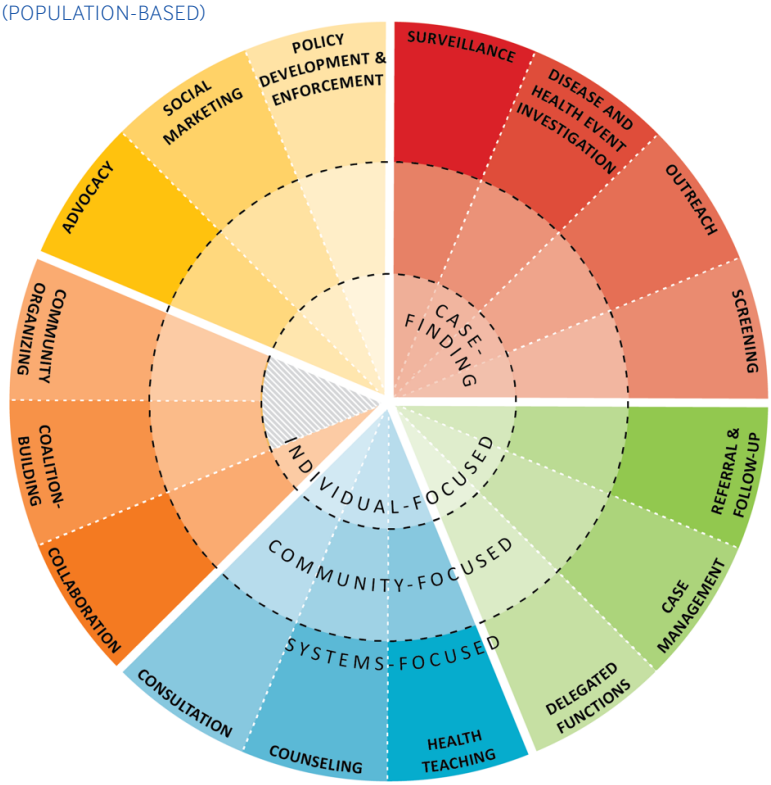
2. Intervention: what do you want to do together?

Your goal for sharing data might be to design a health intervention, rather than just evaluate the health of a community. You'll need to start by outlining the proposed mechanisms you will use to achieve the health outcome goals. There are various types of interventions and levels of practice, some of which are summarized in the Public Health Interventions wheel, shown in the diagram below.

The wheel is a population-based practice mode. It includes sixteen public health interventions and three levels of practice: individual/family, community, and systems.[iv] This tool was originally developed to describe public health nursing practice. However, we can broadly apply it to health interventions in multi-sector data-sharing projects, and we can also incorporate healthcare and social services.

It's important to describe your proposed intervention along with the intended level of practice. This matters because the level of practice you chose may dictate whether the data you need should be identifiable or not – and if so, to what degree. Consider what level of data granularity you will need for each intervention, and what the potential data sources might be. Be mindful of these considerations, since they will impact how you conduct your legal analysis.

PUBLIC HEALTH INTERVENTIONS
(POPULATION-BASED)



Individual/family practice: This level focuses on individuals, either alone or part of a family, class, or group. The goal of your intervention at this level is to change the knowledge, attitudes, beliefs, practices, and behaviors of individuals to improve their health and well-being. Some individual/family-level interventions include direct service, case management, care coordination, or crisis intervention.[iv] Interventions with individuals will often involve that you collect and share personally identifiable health information. It is no surprise that this type of sensitive data is subject to strong legal protections – and it may require the consent of patients prior to sharing data, depending on the specific situation.

Community practice: This level focuses on entire populations within the community or, occasionally, on targeted sub-groups within populations. This type of practice aims to change community norms, attitudes, awareness, practices, and behaviors to improve the health and well-being of community members. Some community-level interventions include surveillance, screening programs, or media campaigns.[iv] Designing community interventions means that you may need to collect and share personally identifiable health information, which will be subject to more stringent legal protections. On the other hand, you may collect anonymized, de-identified, or aggregate data that does not identify specific individuals. This type of data is easier to obtain since they are governed by more permissive laws.

System-level practice: This level focuses on the systems that impact the health of people – as opposed to focusing on individuals or communities. Your goal at this level is to inspire change within organizations, policies, laws, and power structures to improve the health and well-being of people. Your efforts to address and advance equity – especially racial health equity – will depend on system-level interventions. Practices in this domain often include the development of mandated health guidelines, passing legislation that positively impacts population health, or creating an assessment and improvement plan for a service delivery system.[iv] Interventions like this generally do not require sharing personally identifiable health information. Although, there may be instances where this may be necessary. For example, a quality improvement assessment for a healthcare system aimed at decreasing hospital-acquired infections might require the evaluation of individual patient files.

It bears repeating that determining the level of data granularity required for each intervention is crucial.

Click on an icon to see a case study example:

3. Data purpose and uses: what information do you need to share?

Your next step is to evaluate what data you need to achieve your project goals. You also need to determine precisely how you'll use that data. You should identify the specific purpose for sharing data and understand that this purpose will determine whether or not it is a legally permissible disclosure.

Even when you specify an appropriate purpose, if the actual use of the data is not consistent with your previously stated purpose then your intended purpose might not be legally viable. So, make sure that your stated purpose for sharing data is consistent with the proposed use of that data.

EXAMPLE: Your goal may be to collect information in order to increase the proportion of vision screening among preschool children aged 5 years and under in your community. It would not be consistent to use that information to also assess children for mental health conditions – unless that was also specified in the project's stated purpose. If your purpose changes or expands, you must determine, through legal analysis, if that change is permissible under existing agreements. The analysis will also outline any new obligations for the participants, such as obtaining consent or notifying them of the change.

Sometimes it will be necessary to obtain personally identifiable information to achieve your project goals.

EXAMPLE: Your goal may be to offer referrals and individual case management to people with HIV but have fallen out of care. To provide them services, you'll first need to specify which individuals are not currently receiving care. Whether or not you can obtain this type of personally identifiable information will depend on existing relationships and active data-sharing agreements. This will also depend on requirements or limitations that exist within applicable laws, conditions that will be determined later during the legal analysis.

You should also define the minimum amount of information you need to achieve your project goals. Some laws may impose a minimum necessary standard[1] and only allow you to disclose information that is necessary to satisfy a particular purpose and only for certain types of data sharing.

But even if you don't face restrictions like these, it is still important to distinguish essential from inessential data. You may be tempted to obtain as much information as possible on any health issue because it could provide greater insight into the matter. But there are real dangers in having too much data, both from a legal and programmatic standpoint.

EXAMPLE: It's possible that you may not be able to process all the data you have in a meaningful way. Perhaps, your project's progress slows down because you are processing data that is not core to your project's goals. In addition, you will need to comply with any legal conditions regarding data protection when it's stored, used, or transferred. Having extra, unnecessary data could significantly increase your project's administrative burden for ensuring compliance with data security standards and could expose your project to greater legal liability in the case of a data breach.

Click on an icon to see a case study example:

4. Data sources and types: where will the data come from?

Once you have identified the information necessary to reach your project's objectives, the next step is to differentiate the types of data that will be involved in your project along with potential data sources. Additionally, you should consider which sources will allow you to most easily obtain the data you need.

POSSIBLE DATA TYPES:	POTENTIAL DATA SOURCES:	POSSIBLE DATA SHARING:
Clinical data	Healthcare providers	Within a single agency
Public health data	Public health agencies	Between agencies at one level or multiple levels of government
Education data	Schools	
Social service agency data	Social service agencies	Between public and private organizations
Environmental surveillance data	Health and community information exchanges	Between organizations in one sector or multiple sectors
	Public dataset	

1 Under HIPAA, the minimum necessary standard means that the provider must make a reasonable effort to limit the disclosure of patient information to only the minimum amount that is necessary to accomplish the purpose of the request. While HIPAA has a "minimum necessary" standard, when a disclosure is made for public health activities and purposes pursuant to 45 CFR 164.512(b), a covered entity may reasonably rely on the representations of a public official that the amount of protected health information requested is the minimum necessary. See 45 CFR 164.514(d)(3)(iii)(A).

Data sharing may occur among the following: programs within a single agency, agencies at one level or multiple levels of government, public and private organizations, or organizations in one sector or multiple sectors. Note that sharing data within a single government agency may be easier than sharing outside of that agency, since a single agreement might cover multiple offices within that agency. Data sharing projects often will include more than one of these arrangements.

Also note that laws often regulate data sharing based on data types or sources, which makes identifying them that much more important. The Health Insurance Portability and Accountability Act (HIPAA) is one such law – it regulates the use and disclosure of protected health information (PHI) in healthcare treatment, payment, and operations utilized by covered entities, namely, agencies and organizations that are covered under the law. The law also defines which covered entities are subject to prerequisites, requirements, and limitations.

Another common federal privacy law that regulates data sharing is the Family Educational Rights and Privacy Act (FERPA),[v] which protects the privacy of student education records. Or take 42 CFR Part 2[vi] that protects the privacy of substance use disorder patient records. Identifying data types and sources of data will be crucial in conducting a comprehensive legal analysis. Ultimately, this will make it easier for your project to put together data requests.

For information on additional federal privacy laws, see The Network for Public Health Law's collection of legal snapshots. Each snapshot provides an overview of basic legal requirements of different federal data protection laws to help you understand how they might apply to a proposed data activity.

Click on an icon to see a case study example:

5. Data elements: what will you need?

Once you have established what data is necessary for your project, you will need to describe the specific data elements that will be exchanged. These elements will vary based on your project goals.

EXAMPLE: Consider trying to identify specific locations in a community where elderly individuals sustain fall injuries. In this case, you'll need exact location data, such as an address and a description of the fall hazard.

You should also differentiate data elements critical to your project goals from those that are desired but optional. An environmental scan that includes peer-reviewed, published research and information on similar projects may help you decide what data elements you really need. It will also demonstrate legitimacy for the need with your data-sharing partners. As you consider what data elements to include, know that those pertaining to personally identifiable information may increase legal requirements for data sharing.

Below is a sample chart that identifies a project's proposed data elements and links them to potential data sources. Remember, some sources have fewer legal limitations and may be easier to work with. Also, keep in mind if one source's data is easier to obtain than another's, you should consider it even if you potentially may not receive every element you seek.

PROPOSED DATA ELEMENTS	POTENTIAL DATA SOURCES	
	Medicaid enrollment and claims data	Public housing enrollment data
1. Head of household/ applicant last name	✓	✓
2. Head of household/ applicant first name	✓	✓
3. Date of birth	✓	✓
4. Age at application		✓
5. Sex	✓	✓
6. Social security number	✓	✓
7. Alien registration number	✓	✓
8. Unit number and street address	✓	✓
9. Unit city	✓	✓
10. Unit state	✓	✓
11. County	✓	
12. Unit zip code + 4	✓	✓
13. Chronic condition diagnoses	✓	
14. Utilization of healthcare services	✓	

Click on an icon to see a case study example:

6. Transmission and storage: what's the method?

Data sharing requires information to move between two or more physical or virtual locations. Depending on the type of data, laws exist that govern how these transmissions occur and how the data can be stored and secured at either end of the transaction.

Important Considerations:

- Identify the methods of transmission and storage you will use among partners.
- Verify that your team has a complete understanding of any electronic systems in use.
- Meet your organization's security requirements for any electronic systems or methods of transmission or storage. These are based in part on legal or contractual requirements.
- Comply with the terms of any existing legal agreements. This includes meeting additional security requirements tied to any of the project's future agreements.
- Consider whether the format of stored and/or transferred data should be encrypted or unencrypted.
- Consider who has access to data and where it will be stored.
- Consult with your organization's security team, so all appropriate precautions are taken to reduce the risk of a data breach and limit legal liability if one should occur.

Click on an icon to see a case study example:

7. Stakeholders: who's included?

After you narrow down your project's potential data sources, you should confirm all the collaborative partners involved in the proposed data sharing. Most – if not all – of your partners are likely already engaged in the project. But this is also an opportunity to identify additional partners who may be needed to complete the use case, or who will benefit from the project.

In a data-sharing collaboration, you should select your partners based on a shared understanding of the project's health objective and outcome goals. Include any organization that will provide, receive, aggregate, store, translate, or transport data – essentially, any agency that comes in contact with it – regardless of whether that data is personally identifiable or not.

Be sure to list names, types, and any relevant special characteristics of all collaborative partners, and detail the relationships between organizations that are administering or collecting information. Organization types can include public health agencies, healthcare providers, substance use disorder providers, and educational institutions. Special characteristics pertain to a legal status of the organization that will have an effect on data sharing (e.g., HIPAA covered entity status,[vii] 42 CFR Part 2 program or provider,[vi] or FERPA covered educational institutions[viii]). Most organizations will know if they are subject to special characteristics, though the legal analysis should also confirm this.

Click on an icon to see a case study example:

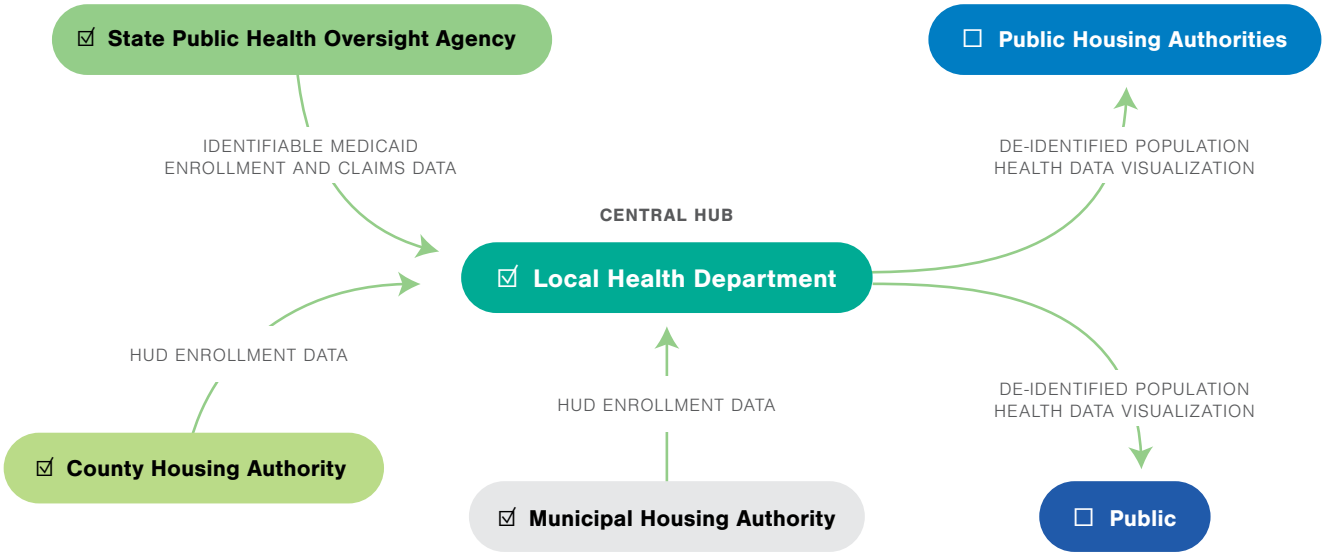
STEP 3

Create a Data Flow Map

Data flow maps are helpful for legal analysis since they identify every point where people and systems interact and where data is transported. That's why devising a data flow map is such a crucial step in developing your data sharing system.

Use process mapping tools to plot out the movement of data within your project from one stakeholder to another. These intersections will have legal consequences, so it is important to make the diagram as complete and accurate as possible.

EXAMPLE: Below is a data flow map that helped to identify every point of intersection for a data-sharing collaborative. The goal of this project was to increase housing security and improve the health and well-being of people.



Click on an icon to see a case study example:

STEP 4

Conduct the Legal Analysis

Once you have developed your use case and established the relevant facts for your project, your attorney will conduct the legal analysis. This is a two-step process where you identify relevant laws, then apply those laws to your data project.

Your attorney will identify all relevant laws that pertain to the organization type, special characteristics, and level of service described in Step 2. Then, they will apply those laws to the design of your proposed data sharing activity to determine its legality.

2 Steps for Legal Analysis

1. Identify the Laws

It's important to reiterate that laws generally regulate data sharing based on the type, source, or proposed use of the data. Data is often subject to both state and federal laws. Some local jurisdictions also have laws regulating specific types of data sharing, though they are much less common.

Generally, federal law overrules state law when their regulations overlap. This rule is known as *preemption*. The exception to this general rule is known as *floor preemption*, and it occurs when federal law provides for a minimum set of standards and specifically allows for state law to create more stringent standards or protections.

The most common example of floor preemption within the data sharing context is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA allows states to adopt data privacy and security standards that go beyond those prescribed within federal HIPAA Privacy and Security Rules.

Cross-jurisdictional data sharing activities will require your attorney to determine how state and federal laws apply to interactions between organizations. The same goes for any data sharing among organizations in different states. Your attorney will identify whether any state laws apply to each partner in the project.

Many states have their own data privacy and security laws, which may subject data to a variety of prereq-uisites, conditions, and limitations. Your attorney will evaluate how these differing standards apply to your project and harmonize any discrepancies. Keep in mind that this may require your project to comply with the legal requirements of the state that has the most restrictive laws.

Laws may be general or specific in nature. A general data law will operate equally upon all types of data within the contexts prescribed by the law. A specific data law will regulate data based on its type, source, or proposed use – and will not apply to all types of data equally. The more specific law will typically prevail when both a general and specific data law apply. Your attorney will be able to determine any exceptions to this general rule.

COMMON TYPES OF DATA LAWS[2]

Health Information	Identity Theft Protection
Public Health Reporting	Patient Rights
Medical Records	Professional Licensing
Data Practices	Facility Certification
Privacy	Insurance Law
Security	Consumer Protection
Breach Notification	Health Information Exchange
Sunshine Law	Social Security Number Protection

2 Though there is no single comprehensive guide to all state and federal data protection laws, the following resource may be helpful in identifying federal laws that are commonly implicated when engaging in cross-sector or cross-jurisdictional data sharing efforts. See "Federal Privacy Laws" at The Network for Public Health Law website.

Once all relevant laws have been identified, your attorney will need to review them to see if your proposed data sharing activity is permissible. This step demands careful analysis to determine what each law allows as well as what prerequisites, conditions, or limitations they impose. In some complex scenarios where your project is seeking different data types or data from multiple sources, your attorney will conduct an analysis for each data set, then compare and cross-reference them to determine what data may be legally shared.

Always keep in mind that a law can be vague or unclear at times. Oftentimes, laws fail to keep pace with advances in technology. Perhaps, a law doesn't address recent legal developments.

EXAMPLE: **The Confidentiality Provisions of The Women, Infants, and Children (WIC) Supplemental Nutrition Program permit the Food and Nutrition Service to use and disclose de-identified WIC data. However, the law doesn't define de-identified data or contain a specific standard or method to render identifiable data as de-identified.**[ix]

If a government agency or court has not provided clarification for gray areas of the law, an attorney may be required to interpret the terms within standards of professional judgment. In cases like this, attorneys tend to be more conservative in their interpretation in order to minimize risk and limit legal liability. However, it's essential that you consider a complete evaluation of the risks, given that not sharing data could lead to missed opportunities for improving people's health and well-being. For this reason, you may want to invite an open discussion of whether a less conservative interpretation would better suit your goals.

2. Apply the Laws

Your next step is to figure out how to comply with the laws that apply to your project. Some laws may be highly prescriptive. For example, they may provide detailed privacy standards or specify the exact language for a privacy disclosure. This tends to make it easier to understand and implement a compliance program that meets the legal requirements. In other cases, the law only provides a list of general requirements but does not prescribe a specific method for achieving them.

It will be crucial to engage with your attorney and security team to review potential approaches and ensure legal compliance. Your organization may have a privacy officer whom you can engage as well. The organization designates the privacy officer to develop, implement, and oversee the organization's legal privacy compliance program. It will be important to create a documented compliance plan that all project participants can reference and agree upon.

Work Within the Law When the Law Doesn't Work for You

There will be times when your data-sharing project is legally not permissible. When this happens, your attorney will identify any legal restrictions or conflicts between laws restricting the proposed sharing. Though this may create a barrier to that specific flow of information, it does not mean you have to give up on your plans to use shared data to reach your community health improvement goals. This is when having your attorney fully integrated into your project team is especially helpful – they will help you seek out creative solutions to navigate legal barriers. Again, this will be easier if you engage your attorney in the project from the use case development phase.

There are many potential solutions to overcoming a barrier to data sharing. Before we outline some solutions, note that they may not apply to your particular project. This is not an exhaustive list, so make sure to work closely with your attorney to identify the solutions that are best for your case. Note that some solutions may require you to change your use case and data flow map.

Six Potential Solutions

I. FIND SIMILAR DATA

If data from a certain source cannot be shared due to legal restrictions, there may be other options. Some laws may be less restrictive or allow for additional protections to be implemented so data may be shared.

EXAMPLE: **You may find it easier to obtain identifiable discharge data reported by health facilities to a public health agency than Medicaid claims data – and you might end up with many of the same data elements.**

II. OBTAIN CONSENT

An individual might agree to share their personally identifiable health information even if the law would otherwise prohibit it (e.g., 42 CFR Part 2). Many laws

have specific requirements for obtaining valid consent, so be sure you are complying with them.

EXAMPLE: The Family Educational Rights and Privacy Act (FERPA) is a fairly restrictive law that does not offer a public health exception for obtaining student information from educational institutions. Getting consent from a qualifying student or their parent or guardian will allow the educational institution to share that student's information with an authorized organization.[x] FERPA requires that a valid consent specify the records that may be disclosed, state the purpose of the disclosure, and identify the party or class of parties to whom the disclosure may be made.[xi]

III. USE DE-IDENTIFIED INFORMATION

This may be a viable option if personally identifiable health information is restricted by law. De-identification standards vary between laws, so make sure that you understand which particular standards for each law apply to a specific data set.

EXAMPLE: The de-identification standard of the Health Insurance Portability and Accountability Act (HIPAA) is very specific.[3] Standards in other state and federal laws, however, can be vague. In cases like this, the relevant standard may depend more on agency or entity policy than the law. You may be able to employ different technological methods that allow you to de-identify information while maintaining more of the data's usefulness.

IV. RESTRUCTURE THE RELATIONSHIPS

You might find that a certain law doesn't allow you to share data, or some other barrier could rear its head. When that happens, you can always go back to the drawing board and rethink your partnership strategy. If this option is feasible, it may clear the path for data sharing.

EXAMPLE: A social service agency may not be permitted to obtain personally identifiable health information without individual consent. But an agency can legally receive that information by using a public health exception within the relevant law. The agency can act as a clearinghouse, obtaining and analyzing the data, and providing it to the social service agency in an aggregate or de-identified form that complies with legal requirements. Agencies also possess broad powers to enact policies and programs aimed at protecting public health and well-being. In some cases, a public health agency may be able to use its authority to employ a data use agreement to disclose personally identifiable information to the social services organization if the disclosure is necessary to carry out its public health mission.

EXAMPLE: In cases where the organization wanting to receive protected client data provides care coordination, case management, or social services that directly or indirectly relate to the client's health, written patient consent may not be needed for the provider to release the information to the organization. The consent exception for "treatment" under HIPAA allows protected health information to be shared with those organizations to further the individual's health or mental health. For example, a provider may disclose protected health information (PHI) about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals.[4]

V. REDEFINE YOUR OVERALL APPROACH

Some laws allow for public health or research exceptions. Restructuring your project to fit into such an exception could allow you to collect the data you need. It is important to note that exceptions might also impose restrictions or limitations on the use or disclosure of the data. So, it's important to fully understand how using this solution could affect your project.

EXAMPLE: 42 CFR Part 2 does not provide an exception for public health surveillance activities. However, it does offer an exception for research.[xii] It might make sense to restructure your project to fit within the research exception in order to obtain the data you need. However, this law also imposes restrictions and limitations on data use, potentially limiting the data's utility depending on project goals.

3 For more information regarding HIPAA de-identification standards, see The Network for Public Health Law's "HIPAA Privacy Rule's Safe Harbor De-Identification Method," and "HIPAA Expert Determination De-Identification Method".

4 For more information on this topic, see The Network for Public Health Law's "The (Largely) Unknown HIPAA Privacy Rule Provision that Speeds Access to Social Services".

VI. MODIFY YOUR ORGANIZATION'S STRUCTURE

You may be able to take advantage of a legal provision that allows you to reduce or remove the barrier that's preventing you from sharing or collecting data.

EXAMPLE: HIPAA allows some covered entities to change their HIPAA coverage status, moving from fully covered to a hybrid entity. Hybrid entities designate components within their organization that perform functions covered by HIPAA and separate them from components that do not perform covered functions. This may allow the non-covered components greater freedom in data sharing.[xiii] Alternatively, organizations can stop performing covered functions and will no longer be subject to the law.

Click on an icon to see a case study example:

STEP 5

Establish and Document Agreements for Sharing

Everything is in place now. You've identified your partners. You've developed a use case. You've mapped out the flow of data. And you've conducted a legal analysis to identify all relevant laws. It's time to make it official and put your data-sharing arrangement on paper.

Data Sharing Agreement

Once you have worked through any legal prohibitions on data sharing and forged pathways to achieve your objectives, you'll need to gain consensus with the project stakeholders to establish and document the terms for sharing data.

This is typically accomplished through a data-sharing agreement, or DSA (sometimes referred to as a data use agreement, or DUA). A DSA is a legally enforceable agreement that operationalizes data sharing among different parties, including organizations and individuals, while protecting privacy, confidentiality, and other data rights.

Functions of a DSA:

- Clearly state the legal authority for data sharing.
- Outline the terms agreed upon by the parties for sharing.
- Identify data elements to be shared.
- Provide monitoring and accountability methods to ensure compliance with the terms of the agreement.
- Describe relationships between parties.
- Define the project's purpose and goals and how the proposed data sharing supports them.

The parties should agree to minimum security requirements for all participants. Data recipients may not be directly affected by law that relates to a data provider, but any legal prerequisites, conditions, and limitations should be included in the agreement for compliance purposes. Most importantly, the agreement needs to demonstrate that the proposed data sharing is legal under all applicable laws.

Some complex projects include sharing data among numerous organizations with multiple agreements in place. In cases like this, each agreement should be compliant with all the others. DSAs should also comply with institutional data-sharing policies and any other legally binding agreements.

Memorandum of Understanding

Under certain circumstances, your project may opt for an alternative to a DSA. A memorandum of understanding (MOU) is a non-binding agreement between two or more parties that outlines the terms, scope, and details of a mutual understanding, noting each party's requirements, roles, and responsibilities.

An MOU is generally a tool used by government agencies in cases where parties are not seeking a legal commitment to each other but wish to engage in an agreement of principle. It often avoids a lengthy contract review process and is, therefore, easier to execute than a DSA.

However, MOUs are not legally enforceable. So, parties engaging in such an agreement do not have legal recourse in case of a data breach, improper disclosure of information, or other issues. This leaves the parties to an MOU with fewer legal protections and may expose them to greater liability for breaches initiated by the agreement's other participants.

DSAs and MOUs often share similar terms and provisions. The most common are listed below.

COMMON TERMS USED IN DSA'S/MOU'S

- Parties
- Purpose
- Communications
- Definitions
- Data to be provided (e.g., data elements, frequency, format, method of exchange)
- Privacy and security requirements
- Period of agreement
- Termination

Other Options

There may be instances where additional agreements are required for your project to be in full legal compliance.

EXAMPLE: For certain types of data sharing, the Health Insurance Portability and Accountability Act (HIPAA) will require covered organizations to execute a Business Associate Agreement (BAA). Under HIPAA, a business associate is a person or entity—other than a member of a covered entity's workforce—who performs functions or activities on behalf of, or provides certain services to, a covered entity and allows the business associate access to protected health information. This includes subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. HIPAA requires covered entities to enter into a BAA with their business associates to ensure that the business associates will appropriately safeguard protected health information. A business associate may use or disclose data only as permitted or required by its contract or applicable law.

Click on an icon to see a case study example:

Conclusion

With this document, we have outlined an approach to analyzing data sharing legal issues in an organized and systematic way.

We hope you and your organization can use this framework to identify and apply any relevant laws to your unique situation and determine the best path forward to achieve your data-sharing goals. This document will help your organization develop a robust use case that can be used to perform a legal analysis of your proposed data sharing in order to engage in systematic, routine exchanges of information for the purpose of improving individual and population health outcomes. Feel free to let us at the *All In* community know about your experience using these "Pathways to Yes."

The Network for Public Health Law

The Network for Public Health Law, with support from the Robert Wood Johnson Foundation, is a national nonprofit organization dedicated to advancing the use of law to promote, protect, and improve public health. As knowledgeable, trained issue-spotters, the Network helps organizations and individuals identify legal and policy solutions that will advance their objectives as well as those that could impede their efforts. The Network also helps them understand regulations, access laws, develop policy, and make sound, evidence-based decisions in order to significantly and positively impact the health of their communities.

Data Across Sectors for Health

DASH is led by the Illinois Public Health Institute and the Michigan Public Health Institute with support from the Robert Wood Johnson Foundation. DASH supports alignment among healthcare, public health, and other sectors to systematically compile, share, and use data to understand factors that influence health and develop more effective interventions and policies. DASH and its partners in *All In: Data for Community Health* are creating a body of knowledge to advance this emerging field by identifying and sharing opportunities, barriers, lessons learned, promising practices, and indicators of progress for sharing data and information across and beyond traditional health sectors.

Robert Wood Johnson Foundation

The Robert Wood Johnson Foundation (RWJF), located in Princeton, N.J., is America's largest philanthropic organization dedicated solely to health. Since 1972, RWJF has provided funding, assistance, and research for projects and programs to help people, their families, and their communities be as healthy as possible. RJWF is committed to working alongside others to build a culture of health that provides everyone in America a fair and just opportunity for health and well-being.

References

i van Panhuis, W. G., *et al.* "A Systematic Review of Barriers to Data Sharing in Public Health," BioMed Central Public Health 14 (2014): 1144.

ii O'Mara-Eves, A., Brunton, G., Oliver, S., *et al.* "The effectiveness of community engagement in public health interventions for disadvantaged groups: a meta-analysis." *BMC Public Health* 15, 129 (2015) doi:10.1186/s12889-015-1352-y

iii Jacobson, I., Christerson, M., Jonsson, P., Övergaard, G., *Object-Oriented Software Engineering: A Use Case Driven Approach,* Addison-Wesley, 1992.

iv Minnesota Department of Health. (2019). Public health interventions: Applications for public health nursing practice (2nd ed.).

v 20 U.S.C. § 1232g; 34 CFR § 99

vi 42 CFR § 2

vii 45 CFR §§ 160, 164

viii 34 CFR § 99

ix 7 U.S.C. § 2018; 7 CFR § 246.26

x *Family Educational Rights and Privacy Act (FERPA).* (2021, August 25). U.S. Department of Education. Retrieved April 13, 2022, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

xi 34 CFR § 99.30

xii 42 CFR § 2.52

xiii 45 CFR §160.103

Glossary

Business associate: Under HIPAA, a person or entity—other than a member of a covered entity's workforce—who performs functions or activities on behalf of, or provides certain services to, a covered entity and allows the business associate access to protected health information.

Computational disclosure control: A de-identification method that prevents the formation of direct connections from unidentified data to identifiable data.

Data sharing agreement (DSA): A legally enforceable agreement that operationalizes the sharing of data among different parties, including organizations and individuals, while protecting privacy, confidentiality and other data rights. Also known as a data use agreement (DUA).

Floor preemption: A situation in which a higher authority of law provides for a minimum set of standards and specifically allows for a lower authority of law to create more stringent standards or protections.

Health Insurance Portability and Accountability Act (HIPAA): A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed by healthcare providers, health insurance plans, or clearing house without the patient's consent or knowledge.

Legal pathways: A way to reach a desired result while complying with all legal requirements.

Memorandum of understanding (MOU): A nonbinding agreement between two or more parties that outlines the terms, scope, and details of a mutual understanding, noting each party's requirements, roles, and responsibilities.

Multi-directional data sharing: A system that allows data to move in more than one direction and can be sent and received by multiple data partners.

Personal health information: Identifying information about an individual that relates to the physical or mental health of the individual, including the health history of the individual's family.

Personally identifiable data: Any data that can be used to identify a specific individual, such as a social security number, address, or phone number.

Preemption: A situation in which a higher authority of law will displace the law of a lower authority of law when the two authorities come into conflict.

Protected health information: Under HIPAA, individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Individually identifiable health information relates to the individual's past, present, or future physical or mental health or condition, and includes: demographic data; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual. It identifies the individual, and allows for a reasonable basis to believe the information can be used to identify the individual.

Statistical disclosure control: A de-identification method that includes a wide variety of techniques and prevents the data receiver from inferring identities of individuals.

Unidirectional data sharing: A system that allows data to move in one direction only, from a data provider to a data recipient.

Use case: A model that describes the interaction between a system and the users of that system to produce a valuable outcome.

Appendix

I. Fall Prevention Case Study[1]

Use Case (Pathways to Yes Step 2)

1. Health Objective

This project attempts to reduce the number of falls that result in inpatient hospitalization or emergency department care within the project's target city. The goal is to reduce these falls by one-third over three years. Currently, older adults in the city suffer over 4,000 serious falls that require a visit to the emergency department or hospitalization each year. These falls frequently lead to death, disability, or loss of independence.

Return to "1. Health, well-being, and equity: what's your objective?" on page 5

2. Intervention

The intervention would help the local health department and partners better understand serious falls among older adults, including geographic patterns and other risk factors so that those risks can be addressed.

Return to "2. Intervention: what do you want to do together?" on page 6

3. Data Purpose and Uses

The purpose and use of the data will be to identify problem locations that contribute to a proportionately high number of falls. The project will also investigate the reasons for falls and use the information to advise community partners on where to locate interventions.

Return to "3. Data purpose and uses: what information do you need to share?" on page 7

4. Data Sources and Type

The state health information exchange (HIE) serving the project city is the data source. The HIE serves as the hub of the project by collecting identifiable hospital emergency department data based on ICD10 codes. The HIE curates, summarizes, and visualizes the data in a dashboard and makes that available to the local health department.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides for two methods that can be used to satisfy the Privacy Rule's de-identification standard: Expert Determination and Safe Harbor.

In this case, the HIE is employing the Expert Determination method: they use cell suppression techniques to de-identify the data in order to protect privacy but preserve some of the geographic data so that the location can be identified for intervention.[2]

Return to "4. Data sources and types: where will the data come from?" on page 7

1 While the explanations and analyses in this case study include references to federal and state laws, the applicability of those laws may not be the same to your data sharing project. In particular, the state laws referenced are not "real." They are a mix of actual state laws and are used to support the examples of how to think through legal aspects of the data sharing process. Use these illustrations as informational examples, not as legal advice for your specific data sharing efforts.

2 For additional information on Expert De-identification, see "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" and "HIPAA Expert Determination De-Identification Method".

5. Data Elements

Core Data Elements (de-identified)

- Date of fall
- Location of fall
- ED admission date
- Age of patient
- Patient health outcome

Return to "5. Data elements: what will you need?" on page 8

6. Method of Transmission and Storage

The de-identified data is transmitted securely between the HIE and the local health department using a directed exchange method. The information is sent over the internet in an encrypted, secure, and reliable way through a trusted exchange that is documented in the participation agreement between the HIE and the local health department. It is stored at the local health department in de-identified form and is subject to reasonable security standards for de-identified data.

Return to "6. Transmission and storage: what's the method?" on page 9

7. Stakeholders

The project has a large list of stakeholders. That includes the local health department, the state HIE, the city housing authority, local schools of public health, nursing, pharmacy and medicine, several local health systems, Meals on Wheels, religious organizations, and several other organizations interfacing with the elderly population in the project city.

The only organizations that deal with identifiable data are the local health systems and the state HIE. The local health department analyzes the de-identified information. After that, the information is made available to other program partners, stakeholders, and funders at regular working group meetings.

The collaboration chose the state HIE as the central data hub for data sharing for several reasons.

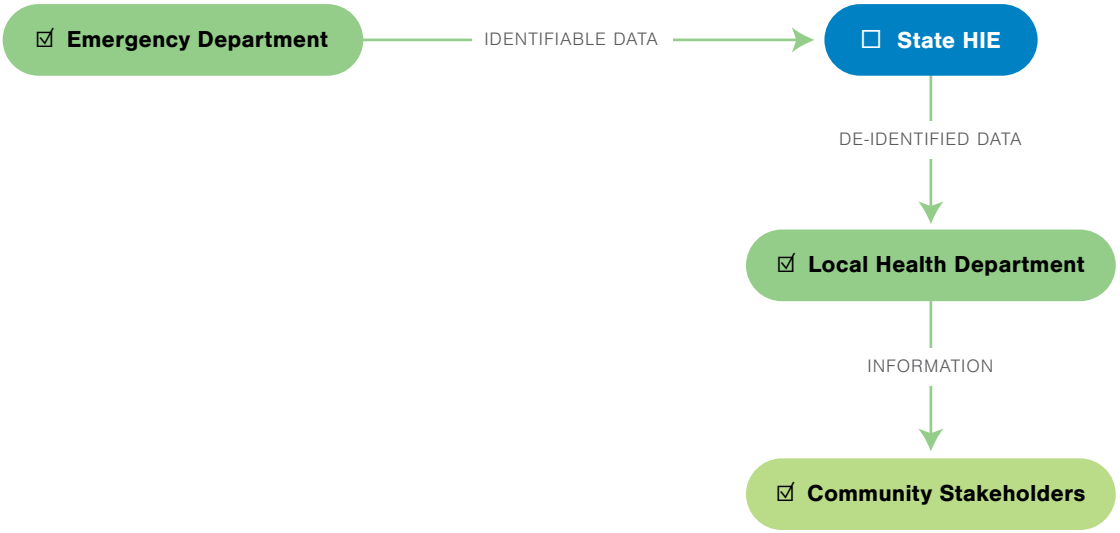
First, as a health information exchange, it already has rules on privacy, security, and breach notification. It complies with all state and federal privacy and security laws.

Second, it has existing relationships with each local hospital and obtains the most accurate real-time source of data on falls. Without existing relationships like this, it is likely the project would never have transpired. It would have taken too long to work with each hospital's legal team to develop the necessary legal agreements.

Third, the HIE already has the capacity to collect, curate, analyze, and visualize the hospital emergency department data.

Return to "7. Stakeholders: who's included?" on page 9

Data Flow Map (Pathways to Yes Step 3)



Return to "Create a Data Flow Map" on page 10

Legal Analysis (Pathways to Yes Step 4)

For this project, only the hospital systems and the state HIE have access to personally identifiable health data. For the legal analysis, it is important to review state and federal privacy and confidentiality laws, as well as state HIE laws, to ensure that the proposed exchange of data is legally permissible.

In the case of this project, the state's privacy and confidentiality law does not apply to de-identified data and therefore would allow the release of the de-identified data to the local health department. The Health Insurance Portability and Accountability Act (HIPAA) is the federal law that governs privacy of identifiable health information. HIPAA, too, allows for the release of de-identified health data as long as the data meets the de-identification requirements specified within the law.

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual – and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

Sections 164.514(b) and (c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard. The Privacy Rule provides two methods by which health information can be designated as de-identified: the Expert Determination method and the Safe Harbor method. As mentioned above, the project is utilizing the Expert Determination method.

The project leadership will have to also ensure that the de-identification method used by the HIE meets any legal prerequisites that state and federal law impose through de-identification standards.

The state's HIE law provides protocols for the release of data for secondary use, including public health practice and research. However, these provisions pertain to identifiable information only.

The state's HIE law does not place any limits on the release of de-identified information by the HIE. This means the proposed data sharing is permissible under state HIE law.

In the project state, consumers may opt out from sharing their information with the state HIE. The project should consider if this is a concern and any effects that opt-outs may have on the integrity of the project data.

Return to "Conduct the Legal Analysis" on page 11

Terms for Sharing (Pathways to Yes Step 5)

The local health department entered into a participation agreement with the state HIE to govern the relationship between the two parties and allows the local health department to participate in the HIE.

Return to “Establish and Document Agreements for Sharing” on page 15

II. Housing and Health Case Study[1]

Use Case (Pathways to Yes Step 2)

1. Health Objective

This project's objective is to provide greater insight into the relationship between housing and health. The goal is to inform, measure and improve future interventions. The project should allow service providers to understand why certain interventions are effective and others are not. Ultimately, the project's purpose is to reinforce the notion that housing is health. It will achieve this by documenting how health outcomes improve when resources are invested in housing and in related services that improve the health of county residents.

Return to "1. Health, well-being, and equity: what's your objective?" on page 5

2. Intervention

This project does not focus on an intervention. It seeks to understand systems-focused connections between housing and health for the sake of future interventions in policy development and collaboration.

Return to "2. Intervention: what do you want to do together?" on page 6

3. Data Purpose and Uses

This project relies on public housing enrollment data and Medicaid enrollment and claims data to develop a longitudinal view. The data needs to include enough personal identifiers, so the project may gain insight into service utilization where target populations overlap. Once the data are linked, system and community level information will be presented to stakeholders and the public.

The project will safeguard individual-level data and will not share it. Individual-level data visibility is not needed for policy development and collaboration.

The project plans to maintain a longitudinal record for future analyses. It will also augment the data with respect to the elderly and to behavioral health. This will be done to obtain a more comprehensive picture of the health of these populations.

Return to "3. Data purpose and uses: what information do you need to share?" on page 7

4. Data Sources and Type

This project relies on personally identifiable administrative data: county and municipal public housing enrollment data, Medicaid enrollment data, and Medicaid claims data. Importantly, the project obtained the Medicaid enrollment and claims data from a state health oversight agency.

Return to "4. Data sources and types: where will the data come from?" on page 7

1 While the explanations and analyses in this case study include references to federal and state laws, the applicability of those laws may not be the same to your data sharing project. In particular, the state laws referenced are not "real." They are a mix of actual state laws and are used to support the examples of how to think through legal aspects of the data sharing process. Use these illustrations as informational examples, not as legal advice for your specific data sharing efforts.

5. Data Elements by Source

PROPOSED DATA ELEMENTS	POTENTIAL DATA SOURCES	
	Medicaid enrollment and claims data	Public housing enrollment data
1. Head of household/applicant last name[2]	✓	✓
2. Head of household/applicant first name	✓	✓
3. Date of birth	✓	✓
4. Age at application		✓
5. Sex	✓	✓
6. Social security number	✓	✓
7. Alien registration number	✓	✓
8. Unit number and street address	✓	✓
9. Unit city	✓	✓
10. Unit state	✓	✓
11. County	✓	
12. Unit zip code + 4	✓	✓
13. Chronic condition diagnoses	✓	
14. Utilization of healthcare services	✓	

Return to "5. Data elements: what will you need?" on page 8

6. Method of Transmission and Storage

The state health oversight agency, municipal housing agency and county housing agency securely transmitted their data to the county public health department's server using Secure File Transfer Protocol (SFTP). The identifiable data are encrypted at rest and secured to the Health Insurance Portability and Accountability Act's Security Standards, 45 CFR § 164.302 *et seq*.

While the county health department's epidemiologist is not covered by HIPAA, the health department is a HIPAA hybrid entity (partially covered by HIPAA) because it provides health services through its clinic and bills for those services electronically. Accordingly, the county health department has elected to secure all of the data in compliance with the HIPAA Security Standard.

Return to "6. Transmission and storage: what's the method?" on page 9

7. Stakeholders

Stakeholders include the county housing authority, municipal housing authority, state health oversight agency, county health department, and the public.

The collaboration chose the health department as the central data hub for several reasons.

First, as a HIPAA hybrid entity, the health department is equipped to handle and protect sensitive health data.

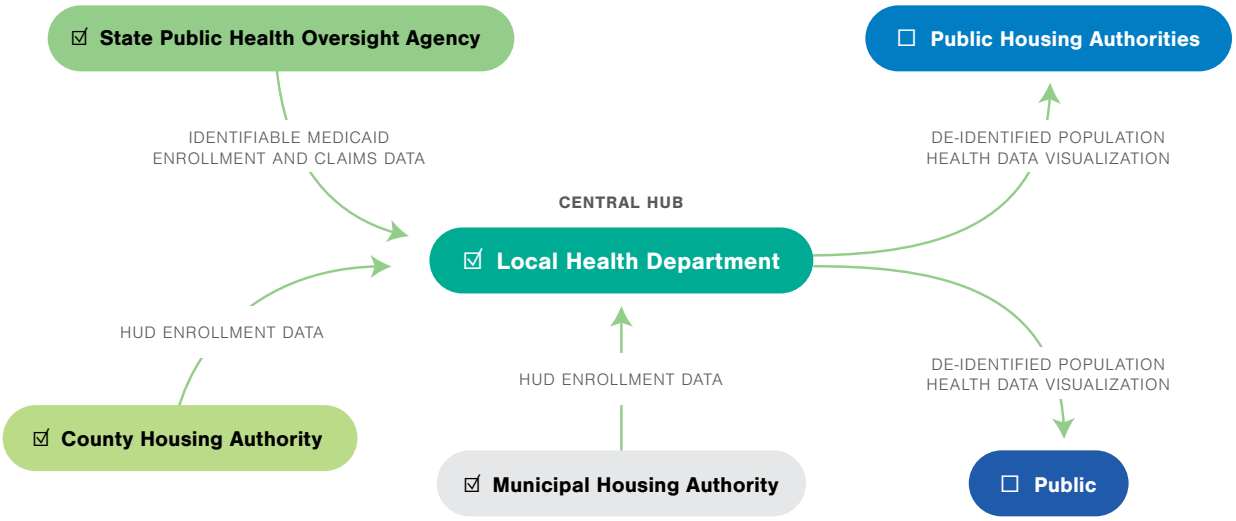
Second, the health department has internal capacity to analyze and interpret the data.

Third, the health department is collecting the data for population health surveillance rather than research purposes. This means it can generally hold data long enough to conduct longitudinal population health studies. In contrast, an entity that collects data for research purposes may have to destroy the data within a shorter time period.

Return to "7. Stakeholders: who's included?" on page 9

2 Demographic information represented in fields 11 – 12, for other household members, is also collected within public housing and Medicaid datasets.

Data Flow Map (Pathways to Yes Step 3)



Return to "Create a Data Flow Map" on page 10

Legal Analysis (Pathways to Yes Step 4)

The state health oversight agency is required by law to collect Medicaid enrollment and claims data from the state Medicaid agency and keep it confidential. State law requires the state health oversight agency to safeguard the data that it receives and protect the privacy of the individuals represented within the data.

The project may not have been able to obtain Medicaid data from the state Medicaid agency, as it is subject to federal law (Medicaid Applicant and Beneficiary Information Safeguards), which limits Medicaid's sharing of applicant and beneficiary information to purposes directly related to plan administration.[3]

State law governs data sharing by the state health oversight agency with the county health department. State law allows data sharing for purposes of health system review as long as confidentiality is maintained. State law allows the health oversight agency to share identifiable Medicaid data with a public health authority where it is needed for a legitimate purpose and privacy is protected. These data were shared under a data use agreement.

The public housing authorities were unclear whether federal law requires consent for the release of identifiable public housing enrollment data. Because this was deemed a gray area, the public housing authorities revised a lease provision to inform tenants of the data elements that would be shared with the county health department. They obtained tenants' consent in the lease signing. The lease revision was intended to build public trust and assure transparency.

Return to "Conduct the Legal Analysis" on page 11

Terms for Sharing (Pathways to Yes Step 5)

The state health oversight agency and the public housing authorities each executed a data use agreement with the county health department to provide for the confidentiality and security of the data.

Return to "Establish and Document Agreements for Sharing" on page 15

3 Medicaid Applicant and Beneficiary Information Safeguards. 42 U.S.C. § 1396a(a)(7); 42 CFR Part 431, Subpart F. See also, the Network for Public Health Law's Medicaid Applicant and Beneficiary Information Safeguards Snapshot.

III. Incarcerated Individuals and Behavioral Health Case Study[1]

Use Case (Pathways to Yes Step 2)

1. Health Objective

This project examines gaps or failures in safety net services provided to people who are both high utilizers of local jails and who have a behavioral health condition (mental health condition or substance use disorder). The project is based on a hypothesis that many individuals who are involved in the criminal justice system are there because safety-net programs do not properly serve them. The project recognizes jails and hospitals as institutions of last resort and seeks to redirect resources to prevent crises through enhanced safety-net service delivery.

Return to "1. Health, well-being, and equity: what's your objective?" on page 5

2. Intervention

This project does not involve the implementation of an intervention. Rather, it is focused on gathering data to inform interventions that may be implemented at the community and systems levels.

Return to "2. Intervention: what do you want to do together?" on page 6

3. Data Purpose and Uses

The purpose and use of the data is to understand and improve the ways in which local safety net programs serve (or fail to serve) individuals who have mental health conditions or substance use disorders and who are frequently jailed (i.e., individuals experiencing four or more jail bookings in a calendar year).

The data must be identifiable in order to match it across data sets. However, once matched, the data no longer needs to be identifiable for purposes of analyzing and reporting to stakeholders.

Return to "3. Data purpose and uses: what information do you need to share?" on page 7

4. Data Sources and Type

The project requires the following types of data:

- county and city jail and court records to identify individuals with four or more jail bookings in a calendar year;
- jail health services records to identify individuals with mental health or substance use disorder diagnoses;
- mental health and substance use treatment records to further understand the nature and treatment of individuals' mental health conditions or substance use disorders; and
- social service records to reveal the use of safety net services and the gaps in those services.

Return to "4. Data sources and types: where will the data come from?" on page 7

1 While the explanations and analyses in this case study include references to federal and state laws, the applicability of those laws may not be the same to your data sharing project. In particular, the state laws referenced are not "real." They are a mix of actual state laws and are used to support the examples of how to think through legal aspects of the data sharing process. Use these illustrations as informational examples, not as legal advice for your specific data sharing efforts.

5. Data Elements

DATA ELEMENT	DATA SOURCE
Demographic data (name, date of birth, gender, race)	County Department of Criminal Justice
Criminal charge information (type of crime, offense type, charge date, status)	
Booking information (booking date, release date	
Drug use or mental health problem reported	
Patient name and date of birth	Jail Health Services - Electronic Health Record (held at County Department of Public Health)
Number of admissions in specified year	
Behavioral health concerns & diagnoses	
Chemical dependence concerns, diagnoses, and detoxification	
Referred for inpatient/outpatient SUD treatment while in jail	
Acute or chronic medical diagnoses	
Mental health treatment	Behavioral Health Division (housed at Department of Human Services)
Substance use disorder treatment	
Jail linkage services (e.g., health care release planning, re-entry case management)	
Specialty court involvement	
Supported housing	
Medicaid coverage	Provider eligibility records (housed at Department of Human Services)
Homelessness status	Homeless Management Information System (HMIS) (housed at Department of Human Services)
Housing type	

Return to "5. Data elements: what will you need?" on page 8

6. Method of Transmission and Storage

The county Department of Criminal Justice (DCJ) and Department of Human Services (DHS) engaged in a Memorandum of Understanding (MOU) under which DHS agreed to perform program evaluation for the DCJ. Under the terms of the MOU, DCJ provides data to DHS via a compact disc (CD). The data is to be promptly transferred to the DHS secured network, after which the CD must be destroyed. Data is to be stored in a subdirectory of the DHS network to which access is restricted to staff who are directly involved with DCJ program evaluation and who have signed a DCJ data confidentiality agreement.

An MOU documents the method of transmission and storage for data shared between the DHS and Department of Public Health (DPH). The agencies share data via a DHS network fileshare created specifically for the project. Access to the fileshare is limited to DHS and DPH staff that are directly involved in the project. These staff members must also complete an annual HIPAA training. Each department's privacy officer manages access to the fileshare.

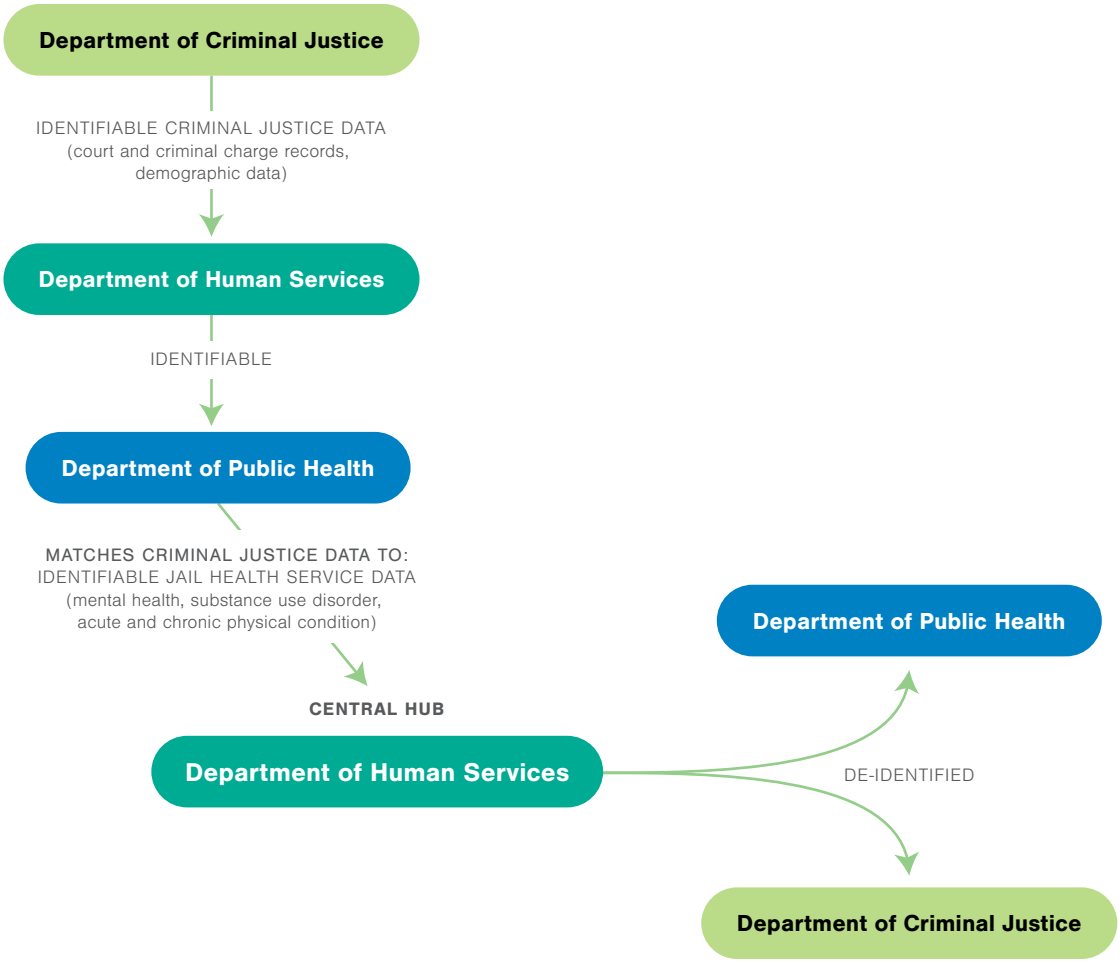
Return to "6. Transmission and storage: what's the method?" on page 9

7. Stakeholders

The primary stakeholders include the county DCJ (including county courts and jails), municipal jails, the DHS (including the Behavioral Health Division and Homeless Services program), and the DPH (including Jail Health Services). The DHS and DPH were the primary partners in developing and executing the project, even though aggregate information and findings were ultimately shared with other stakeholders.

Return to "7. Stakeholders: who's included?" on page 9

Data Flow Map (Pathways to Yes Step 3)



Return to "Create a Data Flow Map" on page 10

Legal Analysis (Pathways to Yes Step 4)

The Department of Criminal Justice (DCJ) is subject to the state's criminal records confidentiality act. The Department of Human Services (DHS) and Department of Public Health (DPH) are subject to the federal Health Insurance Portability and Accountability Act (HIPAA), as they are both covered health care providers.

In addition, both DHS and DPH are subject to the state's medical record privacy act. DHS is also subject to 42 CFR Part 2, Confidentiality of Substance Use Disorder Patient Records, since the DHS is a federally supported substance use disorder treatment provider.

Of the three primary stakeholders involved in this project, DHS is subject to the most stringent data protections because it is covered by 42 CFR Part 2. Under 42 CFR Part 2, there are only limited

circumstances under which identifiable data can be shared without patient consent. These circumstances do not include the program evaluation and quality improvement purposes contemplated in this project. *42 § CFR 2.51-53*.

For this reason, the project designated DHS as the central hub for gathering data and is the only entity with access to the complete set of identifiable data. DHS shares de-identified data back to DPH, DCJ, and other community partners to guide program improvement.

To match multiple relevant data sets, DHS needs to obtain identifiable data from DCJ and DPH. As noted above, DCJ is subject to state law that pertains to confidentiality of criminal records. The law generally permits release of conviction data but limits disclosure of non-conviction data. However, the law allows for the release of both conviction and non-conviction data to individuals or agencies for research, evaluation, and statistical purposes.

The data received from DCJ may be shared, but only pursuant to an agreement with the criminal justice agency. The agreement should provide for certain conditions, such as limiting the use of identifiable information to the permitted purposes and notifying the recipient agency that the records are subject to the state law.

As a provider of jail health services, DPH is subject to HIPAA and to the state medical record privacy law. The HIPAA Privacy Rule permits a covered entity to disclose protected health information (PHI) to another covered entity if both entities have or had a relationship with the subject of the record and the information pertains to that relationship, and the purpose for the disclosure is to conduct health care operations activities. *45 CFR § 164.506(c)(4)*. Health care operations activities include conducting quality assessment and improvement activities and conducting population-based activities that relate to improving health and reducing health care costs. *45 CFR § 164.501*. The state medical record privacy law contains a similar provision.

When a covered entity uses or discloses data under 45 CFR § 164.506(c)(4), it must "make reasonable efforts" to use or disclose only the minimum necessary data for the intended purpose. *45 CFR § 164.502(b).* Ensuring that this project carefully structures the flow of data can facilitate compliance with this requirement.

There are two selection criteria for this project: four or more jail bookings in the last year; and a mental health diagnosis or substance use disorder. For this reason, DPH can assure the disclosure of the minimum necessary information (i.e., information about qualifying individuals only) by providing health data for only those individuals who have already satisfied the first criteria (four or more jail bookings) based on criminal justice records. *45 CFR § 164.514(d)(3)*.

Return to "Conduct the Legal Analysis" on page 11

Terms for Sharing (Pathways to Yes Step 5)

The Department of Criminal Justice (DCJ) and the Department of Human Services (DHS) executed a Memorandum of Understanding (MOU) that allows DCJ to disclose data to DHS for program evaluation purposes. The MOU specifies applicable conditions as required under the state criminal records confidentiality law.

DHS and the Department of Public Health (DPH) also executed an MOU that memorializes the responsibilities of both agencies, demonstrates compliance with applicable laws, and outlines confidentiality and security requirements.

Return to "Establish and Document Agreements for Sharing" on page 15

IV. Medical-Legal Partnership Case Study[1]

Use Case (Pathways to Yes Step 2)

1. Health Objective

This project is focused on two neighborhoods within a large urban area. Despite the vibrant nature of the neighborhoods, more residents live below the federal poverty line and are unemployed than those in the surrounding areas. Homicide rates are twice that of the surrounding areas. The aim of this project is to address issues of substandard housing, poverty, food insecurity, and a lack of public benefits to help improve the health and overall economic stability of individuals.

Return to "1. Health, well-being, and equity: what's your objective?" on page 5

2. Intervention

This project is a medical-legal partnership that includes three partners: a county hospital system, a legal aid organization, and the local health department. The program intervention is to conduct health risk screens when enrolling new patients, including an analysis of both clinical and social needs. If a care coordinator at the local county hospital system identifies a "health-harming legal need," they may either consult with the civil legal aid attorney or refer the patient to the attorney for direct services (advice or representation).

Return to "2. Intervention: what do you want to do together?" on page 6

3. Data Purpose and Uses

The purpose and use of the data are to identify health-harming legal needs, refer patients to direct legal services, and provide attorneys with necessary information to assist patients with their cases.

Return to "3. Data purpose and uses: what information do you need to share?" on page 7

4. Data Sources and Type

The data shared within this medical-legal partnership is fairly limited. In many cases, the care coordinator describes a situation to the civil legal aid attorney. This is so that the aid attorney can provide guidance to the care coordinator on how to assist a patient. In this event, the care coordinator does not share any personally identifying information about the patient.

If a legal need is one which requires attorney intervention, however, the care coordinator requests the patient's consent to share information from the screening with the legal aid attorney.

An authorization form compliant with the Health Insurance Portability and Accountability Act (HIPAA), which must be signed by the patient for the referral to be made, includes the patient's contact information, and it documents the legal needs identified. However, it does not include any health diagnoses or other specifically health-related information. With the patient's consent, the form is shared with the legal aid organization, and the legal aid attorney follows up with the patient directly to obtain additional information.

The legal aid organization shares aggregate level data with the county hospital system and the local health department via weekly and quarterly meetings. This may include reporting on the number of cases handled and general trends as well as sharing anonymized anecdotes.

Return to "4. Data sources and types: where will the data come from?" on page 7

1 While the explanations and analyses in this case study include references to federal and state laws, the applicability of those laws may not be the same to your data sharing project. In particular, the state laws referenced are not "real." They are a mix of actual state laws and are used to support the examples of how to think through legal aspects of the data sharing process. Use these illustrations as informational examples, not as legal advice for your specific data sharing efforts.

5. Data Elements

The only data shared between the county hospital system and the legal aid organization in this project are the patient's contact information and a description of the legal needs that have been identified. The legal aid attorney obtains all other information directly from the patient.

Return to "5. Data elements: what will you need?" on page 8

6. Method of Transmission and Storage

Patient information is transmitted and stored in compliance with the privacy and security requirements of HIPAA. The project has identified and analyzed potential risks to protected health information and implemented security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

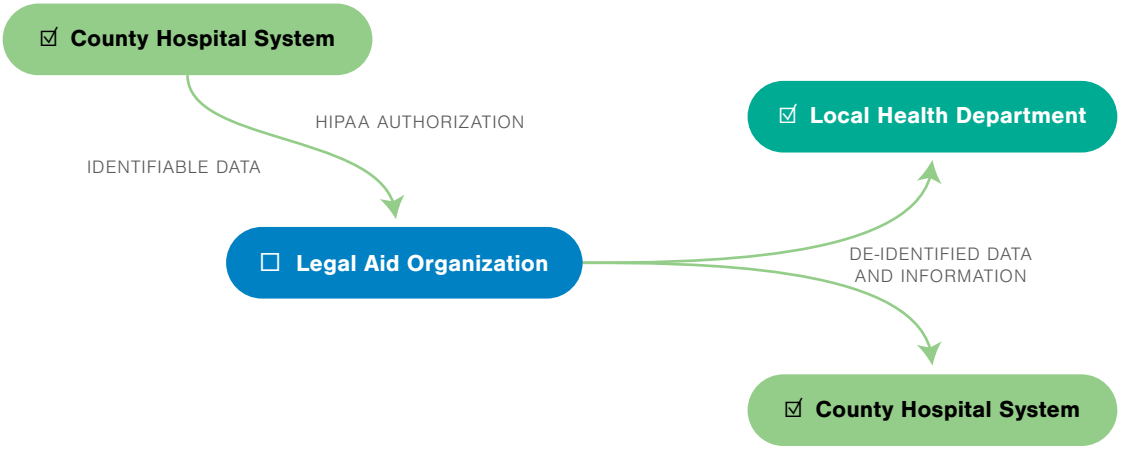
Return to "6. Transmission and storage: what's the method?" on page 9

7. Stakeholders

This project has three stakeholders: the county hospital system, the legal aid organization, and the local health department. All information shared between the county hospital system and the legal aid organization is with patient consent. The three organizations share aggregate level data during weekly and quarterly meetings.

Return to "7. Stakeholders: who's included?" on page 9

Data Flow Map (Pathways to Yes Step 3)



Return to "Create a Data Flow Map" on page 10

Legal Analysis (Pathways to Yes Step 4)

All personally identifiable information is shared within this project with patient consent. HIPAA is a federal law that ensures health information privacy for patients whose health information is held by a covered entity. Patients are required to sign a HIPAA compliant authorization form when providing consent.

The HIPAA Privacy Rule requires an "authorization" for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit the use or disclosure of protected health information unless it is documented with a valid authorization.

An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes (which are generally purposes other than treatment, payment, or health care

operations, since these purposes do not require consent). The authorization also gives covered entities permission to disclose protected health information to a third party specified by the individual. *45 CFR § 164.508*.

The authorization must document specific elements. These include a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date for the authorization, and, in some cases, the purpose for which the information may be used or disclosed. *45 CFR §164.508(c)*. With limited exceptions, covered entities may not condition treatment or insurance coverage on the individual providing an authorization. *45 CFR § 508(b)(4)*.

In the case of this project, state law does not impose any additional requirements for obtaining patient consent. This means the project can operate based on the legal standards set by HIPAA.

For this project, the state's privacy and confidentiality law does not apply to de-identified data. Therefore, the law would allow the release of the aggregate data to the local health department.

HIPAA also allows for the release of de-identified health data as long as that data meets the de-identification requirements specified within the law. In this case, the legal aid organization is not a covered entity under HIPAA. Therefore, the organization is not required to abide by HIPAA standards regarding de-identification of health information. Although, it may still follow such standards if it chooses.

State law does not impose any additional requirements on the sharing of de-identified information by the legal aid organization. Although lawyers have ethical and legal obligations to maintain client confidentiality, they are not prohibited from sharing de-identified information.

Return to "Conduct the Legal Analysis" on page 11

Terms for Sharing (Pathways to Yes Step 5)

The county hospital system has developed an "Authorization to Disclose Protected Health Information" form. The patient completes this form to authorize the county hospital system to share the patient's information with the legal aid organization.

Return to "Establish and Document Agreements for Sharing" on page 15

V. Opioid Misuse Prevention Case Study[1]

Use Case (Pathways to Yes Step 2)

1. Health Objective

The County Opioid Misuse Prevention Initiative (Initiative) was launched in response to the national epidemic of opioid use and a spike in opioid-related deaths in the county. The county health department has provided leadership to engage key stakeholders throughout the community, bringing organizations together to share their experiences, priorities, and outcomes. The Initiative aligned its efforts with the Strategic Prevention Framework[2] and the Sequential Intercept Model.[3] The Substance Abuse and Mental Health Services Administration (SAMHSA) recommends both to facilitate comprehensive approaches that yield positive outcomes.

Return to "1. Health, well-being, and equity: what's your objective?" on page 5

2. Intervention

The health department launched the County Opioid Surveillance System (Surveillance System), in collaboration with several governmental and non-governmental agencies in the area to monitor opioid-related overdose incidences in the community through active surveillance. The surveillance system has provided Initiative members with a complete and fair picture of the opioid crisis in the county, resulting in the development of a strategic plan that encompasses education and awareness, harm reduction and criminal justice, and prescribing practices and prescription drug disposal.

Return to "2. Intervention: what do you want to do together?" on page 6

3. Data Purpose and Uses

The Initiative recognizes that good data are key to understanding the nature and scope of the epidemic, identifying interventions, and measuring what works. Good data are also critical to advocacy and requests to fund programs and services, such as expanded access to naloxone and medication assisted treatment for inmates.

Return to "3. Data purpose and uses: what information do you need to share?" on page 7

4. Data Sources and Type

The health department is a neutral and experienced partner to receive data, provide analyses, develop reports regarding key indicators and trends, and inform the partner organizations and the public about opioid misuse in the county. Supporting the Initiative's goals, members contribute data voluntarily based on each organization's comfort and willingness to share data. The health department receives identifiable data from each source, links the data, shares aggregate de-identified information with partner organizations, and informs the public through monthly reports posted on the health department's website.

Partner organizations have varied in their data contributions. Currently, the primary data providers are the following:

- The county medical examiner office provides information from their investigative reports, including identifiable data, for each death in the county as well as for deaths in surrounding counties of county residents in which any opioid (prescription, non-prescription, or both) alone or in combination with other drugs was present in the system of the decedent.

1 While the explanations and analyses in this case study include references to federal and state laws, the applicability of those laws may not be the same to your data sharing project. In particular, the state laws referenced are not "real." They are a mix of actual state laws and are used to support the examples of how to think through legal aspects of the data sharing process. Use these illustrations as informational examples, not as legal advice for your specific data sharing efforts.

2 Applying the Strategic Prevention Framework (SPF).

3 Data Collection Across the Sequential Intercept Model: Essential Measures.

- Emergency Medical Services (EMS) associated with the city fire department provides information from its electronic records. This includes demographic information and identifiable information collected during the initial on-site assessment of the patient, treatment administered, and use of naloxone.
- Law enforcement agencies in the county and the surrounding areas report the details surrounding opioid overdose deaths and overdose incidents occurring in their jurisdiction.
- The State Syndromic Surveillance System, which the county health department accesses as an authorized user, also provides data. The Syndromic Surveillance System is a web-based reporting system maintained by the state health department to detect communicable disease outbreaks and emerging threats in their early stages. Hospital emergency departments, poison control centers and some urgent care centers generate the data and securely send it to the state. The system is intended to track all complaints, including any overdose and poisoning case, by collecting a patient's basic demographic information (i.e., birth date, gender, zip code of residence) and "chief complaint" (their reason for the visit or call).

The health department would like to receive data from the emergency department of the local hospital concerning individuals who present with overdose-related diagnoses, but the hospital has been reluctant to provide such data, citing the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. As discussed below regarding EMS, the HIPAA Privacy Rule would permit a hospital to share identifiable emergency department data with the health department for public health activities.

Return to "4. Data sources and types: where will the data come from?" on page 7

5. Data Elements

As described above, the health department collects a variety of data from various agencies and sources. They collect data regarding key indicator and trends, including opioid-related mortality, use of Naloxone, drug-overdose incidents, and drug overdose-related transports to the hospital emergency department visits.

Depending on the data source, data might be identifiable (with data elements such as names and birth dates), de-identified (counts of individuals who have suffered an opioid-related overdose), or a limited data set that includes, for example, an individual's date of birth, date of treatment, and zip code of residence.

Identifiable data helps the health department link datasets, so they may understand what is occurring across sectors and over time with respect to the individual. The health department removes identifiers and presents aggregate information to its partners for purposes of planning, intervention, and assessment.

Return to "5. Data elements: what will you need?" on page 8

6. Method of Transmission and Storage

The health department securely receives data through various mechanisms, depending on the capability of the data provider. Most data are transferred to the health department using Secure File Transfer Protocol. Some smaller data files are transferred to the health department by secure (encrypted) email.

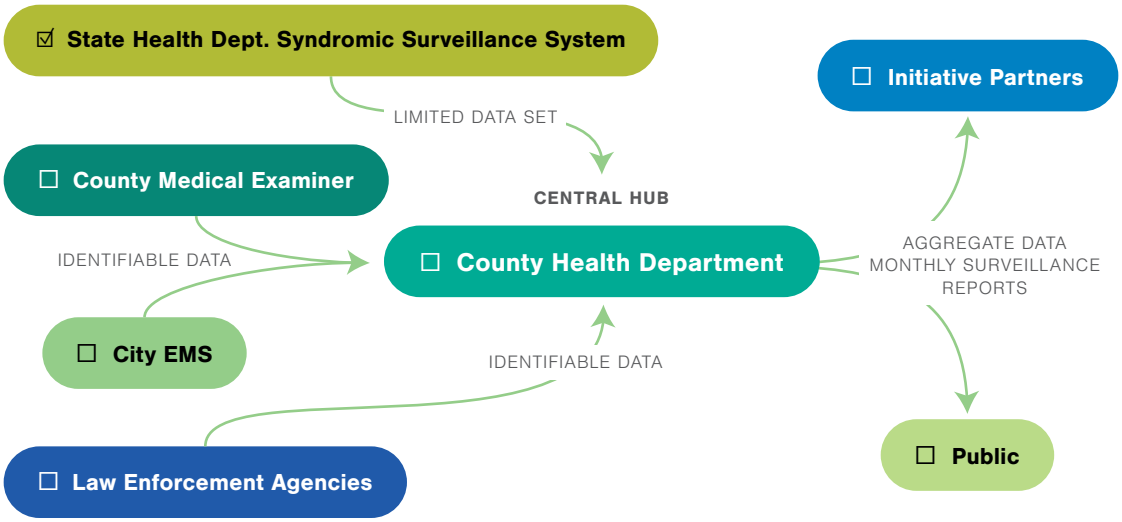
Return to "6. Transmission and storage: what's the method?" on page 9

7. Stakeholders

The Initiative comprises a cross-sector group. The group includes the county health official, law enforcement, emergency medical services, local hospitals and providers, treatment facilities, and community groups that work together to prevent and reduce opioid addiction, overdose, and related harm at all levels and for all ages. The Initiative carries out its work through leadership from the county health department and committees that are focused on different aspects of opioid addiction and overdose prevention.

Return to "7. Stakeholders: who's included?" on page 9

Data Flow Map (Pathways to Yes Step 3)



Return to "Create a Data Flow Map" on page 10

Legal Analysis (Pathways to Yes Step 4)

A variety of laws apply to data sharing, depending on the data source and data type.

State law governs the legality of the medical examiner's data-sharing activities. State law requires the appointment of a county medical examiner to investigate certain types of death such as sudden and unexpected deaths, accidental deaths, and violent deaths. The medical examiner makes a determination of the cause and manner of death and prepares a report with their findings. Generally, these reports are available to the public upon request. Although, the state supreme court has ruled that the medical examiner might withhold a report in some situations where disclosure of the information in the report would amount to a "clearly unwarranted invasion of privacy" of the deceased or their family. Under this initiative, the medical examiner provides information to the county health department, but not to the general public. The health department maintains this information securely and only releases it in aggregate form.

State law governs the legality of data sharing by law enforcement. Generally, police dispatch logs, incident reports, arrest reports, and similar records are available to the public. In limited circumstances, law enforcement may prohibit public access to records that are not of public interest and involve an unwarranted invasion of personal privacy, as interpreted by the courts. Personal privacy concerns are minimized here since the data is being provided to the health department, which releases it only in aggregate form.

Federal law governs the legality of data sharing by Emergency Medical Services (EMS). The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule applies to the EMS. *45 CFR § 160.103*. This is because the EMS electronically transmits standard transactions to health plans in order to obtain payment for services. There is no legal requirement for EMS to provide overdose data to the county health department. However, the health department is authorized to collect and use such information in exercising its general powers and responsibilities to protect the public's health and prevent and control disease and injuries. The HIPAA Privacy Rule permits a covered entity to disclose identifiable health information to a public health authority, without the individual's authorization, for public health purposes including public health surveillance, investigations, interventions, and program evaluation. *45 CFR § 164.512(b)*.

State law governs the legality of sharing state syndromic surveillance information by the state health department. The county health department is authorized to access such data concerning its own county in order to carry out its responsibility to protect the public's health within its jurisdiction.

Return to "Conduct the Legal Analysis" on page 11

Terms for Sharing (Pathways to Yes Step 5)

To address legal concerns, the county health department provided a letter to organizations that are covered by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The letter explains the health department's request for opioid-related information and the legal basis under which the information is requested. Letters like this are valuable for addressing legal concerns since the HIPAA Privacy Rule allows a provider to reasonably rely on a public health authority's statement about its legal authority to collect requested data for public health purposes. *45 CFR §164.514*. Data contributors have signed a data sharing agreement with the health department.

Return to "Establish and Document Agreements for Sharing" on page 15