# Inter-Jurisdictional Health Information Exchange

Guidance for Public Health Agencies

September 2013

JPHIT Joint Public Health Informatics Taskforce

Public Health Informatics Institute

# Table of Contents

*"If names be not correct, language is not in accordance with the truth of things. If language be not in accordance with the truth of things, affairs cannot be carried on to success." ~ Confucius*

# Background

Health information increasingly needs to flow beyond the jurisdiction in which it was originally collected. As both people and microbes move across jurisdictional boundaries with increasing speed and ease, so too must health information.

Historically, health data privacy protections were established by state law. Such laws address issues of allowable disclosures, uses of data, and consent requirements, among other issues. However, the passage of the HIPAA privacy rules established a "floor" of privacy protections and security requirements that superseded less stringent state laws.

With an increased focus on privacy and security regulations comes an increased level of caution and formality related to data exchange between organizations, increasing the use of data exchange/data use agreements to establish clear parameters for exchange.

This paper was created by the Joint Public Health Informatics Task Force (www.jphit.org) to provide practical guidance to public health agencies entering into an inter-jurisdictional, health department-to-health department data exchange relationship. It cites typical provisions for such agreements, why each are important (although not all are needed for every agreement), and practical considerations in crafting each provision. It also includes sample agreements currently in use in different public health domains.

> *This guidance is intended to help prepare you for conversations with your legal counsel and/or privacy officer, who will be the best resource to you in all such activities. Consult with counsel early and often to ensure you develop an agreement that will protect your data and your interests for the life of the agreement.*

# General Guidance

- Every data exchange agreement between two or more entities will be unique in terms of the purposes and the data being exchanged. This brief provides general guidance on common provisions used in such agreements. Not all provisions included below will be needed for every agreement, you may need other provisions not listed below, and the order may not be the most logical for your agreement. Use common sense and critical thinking to craft an agreement that meets your unique needs and audiences. Consider each provision for the clarity, organizational protection, or other value it could provide.
- Talk with legal counsel when you begin creating your agreement; they may have experience crafting similar agreements for other program areas, potentially saving you a lot of work.
- Plan ahead. Reaching agreements on legal documents takes time and can easily stretch into months. It may be helpful to remember that challenges with implementing data exchange are more often related to policies, politics, processes, and people than technology.
- Write in clear, concrete and unambiguous terms.
- Write the agreement as if none of the individuals currently negotiating it will be around for its implementation. That way, you minimize the chance of leaving important issues undocumented in the agreement because "it's understood."

- Cooperation and trust between the jurisdictions are essential. It's been said that health information exchange can only proceed "at the speed of trust."
- All staff who will be working with the data being exchanged should be knowledgeable about the provisions and requirements of all agreements, policies, and statutes governing the data.
- The provisions of an agreement are typically numbered or in outline format. Titles for each provision are also customary.
- Each governmental agency will have a set of provisions that it requires in most, if not all, agreements. The other party will have a similar, but different set of provisions. Ask your legal counsel about how to address the competing boilerplate clauses.
- Each data element and type of data may be subject to differing state, municipal, and federal laws and policies. Consult legal counsel to determine which laws and policies apply to the data being exchanged. For example, vital records and newborn screening data may be subject to different laws and policies than immunization data.
- Ensure written confidentiality and security policies are effective in your jurisdiction to cover all data that is subject to the agreement.
- Agreements may refer to or incorporate policies from one or more jurisdictions. Obtain and review these policies to ensure that there is no conflict with policies in your jurisdiction. Have your legal counsel review all applicable policies from other jurisdictions.
- There may be consent documentation requirements for disclosure or re-disclosure of data. Any such requirements must be explained in detail in the agreement.
- Every governmental agency will have policies concerning the beginning dates and end dates for all agreements. Ask legal counsel for these policies.
- Include contact information of an individual from each of the signatories. These will be the individuals contacted for notices of renewal, amendments, or a termination. Ensure a transfer of responsibility if a designated person leaves that position.
- Make sure legal counsel reviews the final draft version before signatures are attached. Even presumably small changes in wording can have a big legal impact in cases of improper use or disclosure of data.
- Data exchange agreements require ongoing monitoring to ensure compliance.
- Ensure staff who work with personally identifiable data receive regular training on privacy protections.

## Understanding Privacy, Confidentiality, and Security

Although often used interchangeably, the terms privacy, confidentiality, and security have distinct legal and ethical meanings related to identifiable health information.

- *Privacy* refers to rights of an individual to control how information about the individual is collected, used, and disclosed. The value of privacy derives from ethical principles of autonomy that imply individuals are entitled to some level of control over data, including health data, unique and personal to them.
- *Confidentiality* refers to the obligations of individuals or groups who receive or use information to respect the privacy interests of individuals who are the subjects of the data.
- *Security* refers to technologic, physical, or administrative safeguards or tools designed to protect data, including health data, from unwarranted access or disclosure.

# Sample Provisions in Health Data Sharing Agreements

## Parties to the Agreement

**Purpose**

- Indicates which entities are included in the agreement as signatories, and so are legally bound to the provisions of the agreement. The entity named will, in many cases, be the state, county, or city, or the name of the health department for that jurisdiction. Confirm the proper entity with legal counsel. The proper name of the entity will differ in each jurisdiction. For example, in some jurisdictions, the state will be the named entity, but the agreement will be applicable to the health department.

**Guidance**

- Use the full legal name of each entity that is a party to the agreement.
- You may choose to *collectively* refer to the parties as "Trading Partners," "Data Exchange Partners," or a similar term. If so, include a definition of your chosen term (see below). When it comes to defining specific roles and responsibilities of the agency sending data and the one receiving it, consider using terms such as "sending agency" and "receiving agency." Whatever terms you choose to use, define them in the definitions section and use them consistently throughout the document. If the data exchange will be bilateral, it will reduce confusion to use the proper name for each of the entities because each will be a "sending agency" and each will be a "receiving agency."
- Most governmental agencies have a standard way to designate and name signatories and the individuals who are authorized to sign for each agency. Ask your legal counsel how to identify and properly designate these individuals.
- If multiple entities will become parties/signatories to the agreement, consider adding a clause such as, "This agreement will be executed in counterparts representing each party, each of which shall be deemed to be an original, and all such counterparts together shall constitute one and the same agreement." This prevents having to send the same hard copy of the agreement to multiple locations in order to obtain signatures in sequence. Ask your legal counsel if electronic signatures are acceptable, and what, if any, standard for electronic signatures is required.

## Definitions

**Purpose**

- To ensure clear and unambiguous use of terms that are critical to an understanding and enforcement of the agreement.

**Guidance**

- Definitions can be included as a separate section at the beginning of the agreement (such as in statutes) or as footnotes. The number and complexity of the definitions should be your primary guide on which is most appropriate. Footnotes work for relatively few and simple definitions.
- Consider using well established definitions for common terms where possible.
- Include any word that may be subject to differing interpretations. Don't assume all the parties understand terms used in the agreement in the same way.

## Purpose of the Agreement

**Purpose**

- Indicates the specific intentions of the agreement.

**Guidance**

- This provision should clearly answer the question about what public health goal is being addressed, and why the data is being exchanged to help address that goal.
- The purpose could be included in an introductory paragraph rather than as a separate provision in the agreement. This is sometimes handles through the use of a preamble, using a statement such as, "Whereas the parties to this agreement share a common public health interest in …"

## Responsibilities of the Parties

**Purpose**

- Specifies the responsibilities of each party so that duties and expectations are clear.

**Guidance**

- The level of specificity for this provision will depend largely upon how many other provisions are included that address issues such as the data elements, timing, frequency, method of exchange, authority to exchange, etc. For instance, the agreement could have one large provision of numbered responsibilities that include many of the provisions discussed below. Or an introductory sentence could state that the parties "agree to abide by the provisions of this agreement," then go on to list the provisions in separate numbered paragraphs.
- You may choose to use terms such as "Sending Agency (or Entity or Partner)" and "Receiving Agency (or Entity or Partner)" as a way to more clearly specify responsibilities by role (realizing that any given entity could be both a sender and a receiver at different times). Be sure to always use such terms consistently throughout the document. See also guidance under the Parties to the Agreement section.

## Authority to Exchange

**Purpose**

- Identifies the statutory or other authority/authorities for the parties to (1) enter into the agreement, and (2) exchange health information.

**Guidance**

- It is best to cite specific state statutes for each of the parties. Do not use generic language such as, "Information exchanged under this agreement is governed by the applicable state statutes of the Parties."

## Data to be Exchanged

**Purpose**

- To specify what information or data elements may be disclosed from one party to another under this agreement. The format of the data may also be specified, including particular standards. You may also include what information may *not* be disclosed.

**Guidance**

- If a nationally accepted data set exists, you may choose to simply reference that. Consider using generic language such as, "… the most recently published core data set as approved by CDC," so that you do not have to amend the agreement if the data set is updated. Alternatively, you can include an appendix that lists each data element (including the data format, and whether each

element is required, recommended or optional), with a provision that says the appendix can be amended without amending the entire agreement. The route you choose might be based on the number and complexity of the data set standard, how often it changes, whether there is an authoritative source that maintains and publishes the standards, etc.

- If the data elements are established in a statute or rule, it is prudent to list them in the agreement (versus citing the source statute), since it helps to ensure understanding of and compliance with the law.
- If a nationally accepted standard exists for the data format, reference it, or include it in an appendix, in a similar way as above. Adhering to such standards helps to minimize staff time in transforming data.
- Consider whether you need or want to specify the transport protocol to be used by the parties.
- Be sure to have your IT department and/or vendor review the draft language on data elements, formats, and transport. This ensures your information system and IT infrastructure can support the provisions of the agreement.
- If the information being disclosed is identifiable data—that is, the data includes sufficient information that you could identify an individual—explicitly state that so it is brought to the attention of all parties. Consult with legal counsel and your HIPAA privacy officer to learn if your agency is a Covered Entity (or Hybrid Entity) under HIPAA and if the data exchange is subject to HIPAA. If the data disclosure is required or authorized by state law, some provisions of HIPAA may not apply. Consult with your legal counsel and HIPAA privacy officer concerning requirements of HIPAA.
- If named data is to be exchanged, and if the receiving agency may be matching and merging individual records, ensure you are including enough demographic or other data to ensure accurate matches. Listing the required data elements in an appendix (see above) will help ensure accurate record matching.
- The data being exchanged may be based on the residence of the individuals; for instance, a state sending birth record or immunization information for someone born or receiving healthcare in one state but living in another. In such cases, the agreement can specify that information on non-residents will be sent to the jurisdiction of residence on record. Such exchanges are most often done on a scheduled frequency (see Timing of Exchange below).

## Allowable Uses

**Purpose**

- To clearly define what uses the data can be put to by the receiving entity. Any other uses would generally be considered a violation of the agreement, and potentially a breach of confidentiality subject to penalties of the laws of the sending entity and likely the receiving entity as well.

**Guidance**

- Using clear, unambiguous language is especially important in this provision.
- Each use permitted by the agreement must generally be in compliance with the laws and policies of both or multiple states, although this is a matter of interpretation. A receiving state could take the position that data is subject solely to its laws and policies. Permitted uses of the data and the applicability of each state's laws and policies to define those permitted uses is an important area that needs to be clearly stated in the agreement.
- Possible allowable uses include statistical analysis to create more complete records on a person(s), providing case information to public health programs to enable appropriate interventions, public health surveillance, linking with appropriate databases, research, program evaluation, and community health assessment. The allowable uses will largely be determined by programmatic goals and state and federal laws and policies.
- While it is likely not feasible to list all known *unallowable* uses of the data by the receiving entity, consider whether to include any unallowable use that is of particular concern to you.

- If the data can be re-disclosed by the receiving entity, include any requirements for such disclosure, including the persons and/or entities to whom the data can be re-disclosed, the permissible uses for the data that is re-disclosed, whether a data sharing/data use agreement must be in place and, if so, any specific provisions or limitations that must be cited in the agreement. Be sure to define what constitutes re-disclosure.
- Explicitly state in the agreement that each party agrees to abide by all governing laws, including HIPAA, if applicable. Some jurisdictions choose to abide by the provisions of HIPAA even if it does not govern the jurisdiction or the data that is subject to the agreement.

## Privacy Protections/Confidentiality

**Purpose**

- To make explicit that the confidentiality of the data is to be ensured, and that privacy protections govern the exchange and subsequent uses of the data.

**Guidance**

- This is often done by specifically referencing the applicable state laws of the sending entity. The laws of the receiving entity may also apply to the data, however, this does *not* substitute for precisely specifying the allowable and unallowable/prohibited uses of data (see the previous section).
- Make sure to include a provision that the privacy protections remain in place even after the agreement is terminated.
- Clearly state that your organizations recognize the importance of safeguarding individuals' privacy in exchanging and using health data while simultaneously recognizing a compelling interest on the part of your organization to share health data to prevent, detect, and respond to public health events for the protection of public health and safety.

## Data Ownership

**Purpose**

- To specify whether the sending entity retains ownership of the data, even when held by one or more receiving entities. This is most important when the applicable laws of the sending entity's state persist in governing the uses and disclosures of the data, regardless of who holds the data.

**Guidance**

- If such a data ownership provision is included, it implies that the receiving entities have to be able to flag or log data from another jurisdiction, including which jurisdiction the data came from.

## Timing of Exchange

**Purpose**

- To establish a scheduled frequency for the data exchange, and/or to make explicit that ad hoc queries for records are permissible.

**Guidance**

- If the exchange is occurring as batch files on a routine schedule, for example, of non-residents to the health department of their resident state (see Data to be Exchanged above), state the timing as mutually agreed to by the parties. This could be stated in terms of:
    - Frequency; e.g., weekly, monthly, etc.

    - Timing: e.g., within one day or one week of receipt of a record on a non-resident. This would be used if the data is time-sensitive for the receiving entity.
- If ad hoc queries by the receiving entity for individual or batch records (the latter, as an example, being for information collected within a specified date range) will be allowed, specify any ground rules or limitations to such queries, including who is authorized to make such queries and how they are made (by phone, fax, access to a web-based application, etc.).

## Reporting Violations of the Agreements; Penalties

**Purpose**

- To specify how a receiving entity reports an improper disclosure or use of data that originated in another jurisdiction.

**Guidance**

- Both state and federal law will likely determine penalties; in fact, federal law will always apply. Whether you reiterate the actual potential penalties or simply reference them depends in large part on how much you want all parties to understand the gravity of unauthorized disclosures or breaches of security.
- Include the required timeframe for making such reports, for example, "within two (2) business days of discovering the breach."
- Depending upon the sensitivity of the data being exchanged, you may want to specify security polices and/or procedures. Consult your legal counsel and chief security officer for your agency's security policies.

## Amendments/Addendums

**Purpose**

- Clarifies the process for making additions, subtractions, corrections, or other changes to the agreement (amendments), or supplemental narrative attached to the original agreement (addendums).

**Guidance**

- This can be a general statement, such as, "amendments or addendums can be proposed by either party at any time, and adopted by mutual agreement of the parties," or by specifying a process and timeline for periodic review and updating.
- Generally speaking, you want to avoid too many changes over time, which can create confusion over which provisions apply to what data for what time period, etc.

## Rescinding; Termination

**Purpose**

- To specify how a party or parties may rescind their participation in the agreement and/or terminate the agreement.

**Guidance**

- Specify that notice of rescission must be in writing, and whether the rescission is effective immediately or after a specified time. Also, include if preliminary notice of rescission is required to give the parties time to negotiate, if indicated.
- If the agreement is between only two entities, one of them rescinding effectively terminates the agreement.
- Specify what happens to data that has already been disclosed upon termination by one party. Are data retained by the receiving agency returned or destroyed?

### Dates; Renewal

**Purpose**

- To specify the start date of the agreement and the end date (when and how it expires).

**Guidance**

- Start dates are typically set as an "as of" date. An "as of" date is usually easier to deal with in terms of data exchange and for financial purposes. Alternatively, the start date can be set when the agreement is fully executed; that is, when all signatures are affixed.
- Agreements such as this may or may not have to have a termination date. Your legal counsel can tell you if such agreements automatically expire after a given number of years or at the end of the fiscal period, even if no money is involved. Even if no termination requirements exist, it is prudent to include some provision for periodic review and renewal by the parties.
- Having a specified timeframe for renewal provides an opportunity to update the agreement. For instance, there may be opportunities to add more data elements or adopt new messaging formats or standards for data sharing.

### Signatures

**Purpose**

- To make the agreement binding.

**Guidance**

- Signature lines should include: organization name, name of person signing for the organization, title of person signing the agreement, and date signed.
- Ensure that the person signing the agreement has signature authority for the agency.
- Generally, signatures should be original and in ink, not inserted digital images of a signature. True digital signatures, with security certificates, are becoming more commonplace and may be allowed in your jurisdictions.
- Explore whether an agreement with multiple parties can be signed separately by each of the parties. You may choose—or perhaps be required—to store these separately-signed agreements in a single repository, such as a trade association or the agency that is designated for that purpose, to hold them collectively.

## Sample Data Exchange Agreements

To download the sample agreements, go to www.jphit.org:

- Inter-Jurisdictional Exchange Agreement for Vital Events, 2014-2018
- NAACCR Inter-Registry Resident Data Exchange Agreement
- New York State IIS Data Sharing Agreement
- Inter-State Data Sharing Agreement between the State of Oregon and the State of Washington