

Considerations for Developing Data Sharing Agreements for Your Health Department Data to Care Program

Eve Mokotoff, MPH (HIV Counts)

JSI Consultant

June 12, 2014

This document is intended for internal use only and was produced as part of JSI's CDC-funded contract #200-2009-30955/0005 -- Data to care: Providing technical assistance to state and local public health jurisdictions in their use of HIV surveillance data to support continuous, high-quality care for persons living with HIV.

Learning Objectives

1. Understand the decision process for sharing personally identifiable information on persons living with HIV (PLWH) with agencies outside of the health department
2. Review the “Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality” and understand how to apply them to the decision making process
3. Identify and discuss the essential elements to include in a data sharing agreement

Acronyms/Definitions

- MOU/MOA: Memo(s) of understanding/agreement
- DUA/DSA: Data use/sharing agreement
- S&C: security and confidentiality
- Data to Care (DtC): use of *surveillance data* to identify, locate, link and/or re-engage persons already diagnosed with HIV into adequate medical care

Acronyms/Definitions (continued)

- ASO/CBO: AIDS Service Organization/
Community Based Organization
- Data: aggregate information; for DtC we mean *individual level personally identifiable information*

Acronyms/Definitions (continued)

- Personally identifiable information (PII): Data that can be used to identify, locate, or contact individuals or establishments, or reveal the characteristics or other details about them; and any other information that is linked or linkable to an individual
 - Direct identifiers: name, social security number or other information that is unique to an individual
 - Indirect identifiers: uncommon race, ethnicity, extreme age, unusual occupation and other details, especially in combination with each other or other information

Source: CDC. Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs, 2011.

Questions to be Answered During Today's Webinar

1. How is data sharing defined and used in HIV prevention and care?
2. What principles underlie data sharing?
3. What questions should our HD ask to prepare to share data?
4. Who are our sharing partners and considerations for sharing?
5. What type of DSA should we use and how do we share the data?
6. What are the S&C issues involved with data sharing?
7. What are the essential elements in a DSA?
8. What sample DSAs are available and what sources should we reference for this process?

How is Data Sharing Defined and Used in HIV Surveillance, Prevention and Care?

Allowing minimum access to PII to public health staff or agencies outside of the surveillance unit for specific public health purposes

- Partner/contact management
- Integrated assessment of parallel epidemics or syndemics (TB, hepatitis, STIs)
- Quality of care assurance
- Limited public health research purposes
- ***Engagement with care and treatment assurance***

Data Sharing Agreements

A DSA is defined in the 2011 S&C Guidelines as a “mechanism by which a data requestor and data provider can define the terms of data access that can be granted to requestors”

Principles Underlying PII Sharing

“Despite its critical importance, there is no national standard for safeguarding data held by public health agencies. Instead, privacy safeguards are fragmented across 50 states, creating uncertain and inconsistent privacy protection.”

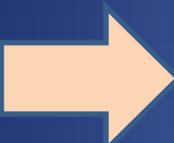
Lee & Gostin. Ethical Collection, Storage and Use of Public Health Data- A proposal for national privacy protection, 2009.

Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality

1.	Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes.
2.	Programs should collect the <u>minimum</u> amount of personally identifiable information necessary to conduct public health activities.
3.	Programs should have strong policies to protect the privacy and security of personally identifiable data.
4.	Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
5.	Programs should have policies and procedures to ensure the quality of any data they collect or use.

Sources: CDC. *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs*, 2011; Lee & Gostin. *JAMA*, 2009.

Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality



6.	Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7.	Programs should share data for legitimate public health purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
8.	Public health data should be maintained in a secure environment and transmitted through secure methods.
9.	<u>Minimize</u> the number of persons and entities granted access to identifiable data.
10.	Program officials should be active, responsible stewards of public health data.

Sources: CDC. *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs*, 2011; Lee & Gostin. *JAMA*, 2009.

Questions to Prepare for Data to Care Activities

1. In order to conduct DtC, will the HD need to share PII from surveillance?
2. Why do we need to share surveillance PII?
3. What specific data elements will we need to share?
4. Who will we share it with?
5. What will they do with the data?
6. Do laws or regulations prohibit or limit this data sharing?
7. What is the experience handling confidential HIV data of the parties who will be accessing HIV surveillance data?
8. Do they currently meet the 2011 S&C guidelines?

Sharing Data Internally/Externally

- Internal sharing (within the HD) is guided first by public health need and then by compliance on the part of all parties with the
- 2011 S&C Guidelines
 - Technical assistance is available by viewing 2013 webinars and tools/examples in the Webinar Library @ CSTE.org
- External sharing (outside the HD) is more challenging and is the focus of today's webinar

Who are the External Partners for Data Sharing?

A valid DtC partner

- Health Care Providers

- ASOs acting on behalf of HD
 - They have been given “public health authority”

ASO as a Data to Care Partner

- ASO that is acting on behalf of the HD has been given “public health authority”
 - Via a contract, DSA, or other legally binding document
- Usually such an agency diagnoses and/or treats HIV infection and has a relationship with the HD
 - Still need a legally binding document

Data Sharing with ASOs

- Sharing surveillance data with ASOs for DtC is dependent on establishing their authority to act as agent of HD
- Role likely limited
- If determined that there is a role, DSA required
- Oversight with initial and ongoing S&C training
- IRB review may potentially be helpful
- Currently no clear examples to draw on

Data Sharing Considerations

- New information on PLWH from *external agency* → *HD*
 - No DSA needed between the HD and external agency
- New information on PLWH from *HD* → *external agency*
 - DSA needed
 - If names originated from HD and are going from HD to external agency and being re-released to a provider network, consider a DSA among all three agencies

MOU? MOA? DUA? DSA?

- The legal meaning of these seems to vary by organization
- Common meanings for HDs include:
 - MOU: statement of principle
 - MOA: specify services/what is being shared
 - DUA/DSA: could include or be an attachment to MOU/MOAs or used more generally to describe any document used as the basis of sharing PII with an agency external to the HD

MOU? MOA? DUA? DSA?

Which Should We Use?

- Which specific template to use will be determined by legal counsel of the organization providing the data (i.e., the PII)
- The organization is usually the HD but secondary release could specify another agency:
 - HD shares data with an external agency (e.g., ASO) that wants to share it with others (e.g., providers)
 - If so, original DSA should either specifically allow or disallow secondary release

How May PII Data be Shared?

Data may be shared:

- Using secure electronic methods (e.g., encrypted file, SFTP) in accordance with S&C Guidelines Standard 5.0
- Over the phone
- Direct contact with surveillance units

How May PII Data NOT be Shared?

- Using paper should be discouraged- it is harder to control access and too easy to leave somewhere
- Never, ever in email, even inside the health department – see Standard 5.3 in the 2011 S&C Guidelines
 - Even though this Standard says emailing unencrypted PII is not allowed the content of email can be subject to Freedom of Information Act (FOI) requests

What Guides the S&C of Data Sharing?

- *State laws/regulations* related to bi-directional sharing of individual-level HIV case surveillance data
- Internal and external agency compliance with *CDC's 2011 S&C Guidelines*

Security and Confidentiality Concerns: State Law

- All data sharing work starts and ends with legal counsel review
 - Understand requirements of state reporting laws and rules/regulations
 - Legal counsel will determine need for
 - MOU/MOA/DSA
 - IRB review can include a DUA – this will probably not be needed for linkage to care activities but it is better to have the discussion beforehand

Security and Confidentiality Concerns: 2011 S&C Guidelines

- The subtitle of this document is “Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action”
- Core principle/value/understanding of the standards in the S&C guidelines is that BOTH the health department and *any organization* with whom a HD shares PII must comply with these guidelines

Security and Confidentiality: our Highest Priority

- Even after a formal agreement has been executed, S&C guideline training should be done upon hire with all new employees and annually
- Training:
 - Can involve changing the culture of a program/agency
 - Content should reference stipulations in the DSA about what can and cannot be done with data being shared

Ongoing S&C Training

- Policies and procedures should model a culture of maintaining the highest level of confidentiality for PII
- HD can assist external agencies with practices to promote this, e.g., placement of confidential fax machines and copiers
 - Training can be:
 - In person (works well when done periodically)
 - Signing off after reviewing a series of slides or a policy

Essential Elements of Data Sharing Agreements

Essential Elements of DSAs

- Once determination is made that a DSA is needed, the following elements should be included:
 - Specific identification of the parties providing data, receiving data and all of those who will have access
 - Purpose of the agreement- what public health goal is being met? Include authority under which sharing is being done for both parties (rules/laws may be different for the two parties)
 - For example, does HIPAA apply to health department and/or the external agency?
 - Roles and responsibilities of all persons with access to data
 - This includes a description of staff training and confidentiality certifications and can/should specify adherence to 2011 S&C Guidelines

Sources: CDC. CSTE Webinar, July 25, 2013 ; JPHI Task Force. Inter-Jurisdictional Health Information Exchange Guidance for Public Health Agencies, September 2013.

Essential Elements of DSAs (continued)

- Description of data to be shared (specific data elements, data formats)
 - Clear unambiguous language is critical
 - Include allowable AND unallowable uses; include any unallowable uses that are of particular concern
 - Include whether the information being shared can be re-disclosed by the receiving party
 - Data ownership- does the HD retain ownership?
- Method(s) data will be shared (how often, how transmitted)

Essential Elements of DSAs (continued)

- Date range data sharing agreement in force and renewal/termination date including procedures for rescinding the agreement
- Specific physical/electronic data security procedures
- Procedures to destroy or remove access to data at termination of DSA
- Process for amendments/addendums
- Notification of breach or misuse of data
- Penalties for non-compliance or violation of agreement terms
- Signatures of certifying officials

The DSA is Complete – What Next?

- Share the data
- Monitor compliance
- Ensure initial and ongoing S&C training
- Amend the DSA as needed
- Renew the DSA or close it out

Samples DSAs

- Texas Data Release Agreement
- Washington state Policy for External Data Sharing
- Louisiana
 - MOA between LDoHH and a CBO
 - DSA between LSU and LDoHH for LaPHIE
 - Affiliation agreement LaCAN Partners/LDoHH
- Michigan Data Sharing Agreement
- NYS Immunization Information Data Exchange

References

- CDC. *Assessment tool for developing the program; steps 5 & 6*. Data to Care Tool Kit. Accessed from: [http://effectiveinterventions.org/Libraries/Data to Care D2C/Assessment Tool PDF.sflb.ashx](http://effectiveinterventions.org/Libraries/Data%20to%20Care%20D2C/Assessment%20Tool%20PDF.sflb.ashx)
- Joint PH Informatics Task Force. *Inter-Jurisdictional Health Information Exchange Guidance for Public Health Agencies*, September 2013. Accessed from: <http://www.phii.org/sites/default/files/resource/pdfs/JPHIT%20Inter-Jurisdictional%20Data%20Exchange%20Guidance%200913.pdf>
- Tipton, Medina. *Kentucky Public Health Webinar: Active Responsible Stewardship: From Training to Responding*, August 26, 2013. Accessed from: <http://www.cste.org/?page=WebinarLibrary>
- Lee, LM & Gostin, LO. Ethical collection, storage, and use of public health data: a proposal for national privacy protection. *JAMA*, 2009; 302:82-84.
- National Institute of Standards and Technology Special Publication 800-34. *Guide To Protecting The Confidentiality of Personally Identifiable Information*.
- CDC. *Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. CDC Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs*, 2011. Accessed from: <http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf>
- Stenger, M. PowerPoint slides: *Driving Public Health with Appropriate Data: Data Sharing – Why, When, Who and How?* July 25, 2013. Accessed from: <http://www.cste.org/?page=WebinarLibrary>



Data Security and Confidentiality Guidelines

for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs:

Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action



National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention



Inter-Jurisdictional Health Information Exchange

Guidance for Public Health Agencies

September 2013



Questions & Discussion