National Human Services Data Consortium

2016 Spring Conference
Los Angeles, CA
April 13-14, 2016

HMIS and Sharing Data: It Seems Complicated but Doesn't Have to Be
Susan Starrett, CSH
Joe Scalise, Info Line, Inc.

Advancing a Technology Culture in Human Services

National Human Services Data Consortium
Advancing a Technology Culture in Human Services

2016 Spring Conference
Los Angeles, CA
April 13-14, 2016

Session Outline

- Data Sharing: What? Why? Who?
- Data Sharing and Privacy Concerns
- Requirements related to Data Sharing and Ensuring Privacy
- Community Example: What not to do and Successful solutions
- Successes and Challenges in Defining the Role of the HMIS
- Discussion

National Human Services Data Consortium
Advancing a Technology Culture in Human Services

2016 Spring Conference
Los Angeles, CA
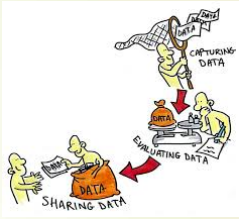April 13-14, 2016

Data Sharing: What?

- Collecting information from an individual or family and sharing that information with others
- Data may be shared in part of in whole
- Data may be shared with some or with all
- Data may be shared across data collection systems (whether it's actually a system or not)
    - If it's not data in HMIS – should it be a concern of the HMIS Lead? CoC?

Levels of Sharing

- Closed – no sharing of data between any agencies
- Partially Open/Closed – some sharing of data between some agencies
- Open – all data is shared between all participating agencies

HMIS Privacy and Security

- Privacy is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.
- Confidentiality pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others without permission in ways that are inconsistent with the understanding of the original disclosure.
- Security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.
- 2004 Technical Standards set forth expectations for privacy and security for HMIS

HMIS Privacy and Security

- Two tiers: required baseline standards and additional recommended protocols;
- Applies to all agencies and programs that record, use, or process Protected Personal Information (PPI) for an HMIS including:
  - Continuum of Care (CoC)
  - Homeless service provider
  - HMIS host or administrator, etc.
- Employees, volunteers, affiliates, contractors, and associates are covered by the privacy standards of the agencies they deal with; and
- Privacy and security standards apply to all agencies- regardless of funding source- who use the HMIS.

National Human Services Data Consortium
Advancing a Technology Culture in Human Services
2016 Spring Conference
Los Angeles, CA
April 13-14, 2016

Data Sharing: Why?

- Ending Homelessness among Sub-Populations
  - Veterans
  - Youth
  - Families
  - Chronics
- Coordinated Entry
- System Performance Measures
- Connecting with Mainstream Resources
- Active Lists
- Coordinating Services

National Human Services Data Consortium
Advancing a Technology Culture in Human Services
2016 Spring Conference
Los Angeles, CA
April 13-14, 2016

Data Sharing: Who?

- Veterans
  - HMIS Participating Veteran Service Organizations
  - Non-HMIS Participating VSO's
- Chronic Homeless
- Youth
- Families
- Domestic Violence
- ?

National Human Services Data Consortium
Advancing a Technology Culture in Human Services
2016 Spring Conference
Los Angeles, CA
April 13-14, 2016

Data Sharing and Privacy Concerns

- Example of Data Sharing/Privacy Breach

- Do we have a release from the client?
- Are all agencies with access to the data on the list of 'sharing' agencies?
- Do all people have access to the data have a signed confidentiality/use agreement signed?
- Are you (HMIS Lead) at the table to discuss data sharing, privacy and security requirements?

- Others?

Data Sharing/Privacy Requirements

- 2004 HMIS Technical Standards
- HMIS Rule (Draft)
- HIPAA
- 42 CFR Part 2
- Local, State and Other Federal Laws

Privacy Standards Framework

- Personal Protected Information (PPI)
  - Includes name, SSN, program entry/exit, zip code of last permanent address, system/program ID, and program type
- Allow for reasonable, responsible data disclosures
- Derived from principles of fair information practices
- Borrowed from Health Insurance Portability and Accountability Act (HIPAA)

Privacy Requirements

- Privacy Standards:
  - Protect client personal information from unauthorized disclosure
  - Seven components:
    - Collection limitations
    - Data quality
    - Purpose and use limitations
    - Openness
    - Access and Correction
    - Accountability

Collection Limitations

- Only collect information that is appropriate for the purposes that the information is obtained or when required by law
- Use lawful and fair means to collect it
- When appropriate, collect data with knowledge or consent of the client
- Post sign; infer consent for collection
  - Must post a sign at intake desk (or comparable location) that explains generally the reasons for collecting this information.

Collection Limitations – Other Stuff You Can Do

- Restrict collection of personal data, other than required HMIS data elements
- Require written client consents
- Obtain oral or written consent from the individual or a third party

Data Quality

- Data must be relevant to the purpose for which it is to be used
- To extent necessary for those purposes, data should be accurate, complete, and timely
- Must develop and implement plan for disposal of Personal Protected Information

Purpose and Use Limitations

- Notice must specify purposes for PPI collections and must describe all uses/disclosures
- A program may use/disclosure PPI only if allowed by the standard and described in the privacy notice
- Notice may infer consent for described uses/ disclosures and for compatible uses/ disclosures
- All uses/disclosures are permissive (except first party request or required by law)
- Uses/disclosures not specified in notice need written consent of the individual or legal requirement

Allowable Uses/Disclosures

- Provide and coordinate services
- Payment or reimbursement
- Administrative functions
- Create de-identified PPI
- Required by law
- Avert serious threat to health/safety
- Academic research (written agreement required)
- Law Enforcement

Purpose and Use Limitation – Other stuff you can do

- Seek oral or written consent for use/disclosure
- Agree to client requested restrictions on use/disclosure
- Limit use/disclosure to those in notice and necessary (not compatible) purposes
- Keep an audit trail for disclosures
- Make audit trails available to the client, if requested
- Limit disclosures to minimum necessary

Openness

- Be open with agencies, client's, and other parties about how you protect client information from unethical use
- You must post a sign about your Privacy policies (called a Privacy Notice) and your Privacy policies must be available to anyone who requests them – including clients and the media.
- If your agency has a web page, you must post your Privacy Notice on your web page. This is true about individual agencies as well as any web pages associated with your HMIS.

Openness – Other Stuff You Can Do

- Provide a simplified copy of your Privacy Notice to clients at the time of data collection.
  - You may need to have copies of your Privacy Notice in more than one language
- Provide advance notice on changes to your Privacy Policy and Notice, how you might enforce those changes, and ask for public comments.

Access and Correction

- Must allow individual to inspect and have a copy of his/her PPI
- Must offer to explain PPI
- Must consider request to correct inaccurate or incomplete PPI
- May deny access to some info
- Must explain denials

National Human Services Data Consortium — Advancing a Technology Culture in Human Services — 2016 Spring Conference — Los Angeles, CA — April 13-14, 2016

Access and Correction – Other stuff you can do

- Allow appeal of denial of access or correction
- Limit grounds for denial of access
- Allow a statement of disagreement
- Provide written explanation for denial

National Human Services Data Consortium — Advancing a Technology Culture in Human Services — 2016 Spring Conference — Los Angeles, CA — April 13-14, 2016

Accountability

- Must establish procedure for accepting and considering complaints about privacy and security policies and practices

- Must require all staff members to sign a confidentiality agreement (acknowledging receipt of and pledging to comply with the privacy notice)

National Human Services Data Consortium — Advancing a Technology Culture in Human Services — 2016 Spring Conference — Los Angeles, CA — April 13-14, 2016

Accountability- Other Stuff You Can Do

- Require formal privacy training
- Regularly audit privacy compliance
- Establish an appeals process for privacy policy complaints and denials of access and correction rights
- Designate chief privacy officer

HMIS and HIPAA

- Health Insurance Portability and Accountability Act (HIPAA) privacy rules take precedence over HMIS Privacy Standards
- HIPAA covered entities are required to meet HIPAA baseline privacy requirements not HMIS
- Most programs are not covered by HIPAA: To learn more go to http://www.hhs.gov/ocr/hipaa/

HMIS and Other Privacy Laws

- Programs must comply with more stringent federal, state and local confidentiality laws; and
- If a conflict exists between state law and the HMIS an official legal opinion on the matter should be prepared by the state's Attorney General and submitted to HUD's General Counsel for Review.
- Domestic Violence Victim Service Providers are prohibited from entering data into HMIS and legal service providers are not to enter confidential client notes into HMIS.

HMIS Consent Models

- Inferred Consent:
  - Baseline Requirement; and
  - Client's consent to release information is inferred from the privacy posting.
- Implied/Informed Consent:
  - Verbal or physical consent is required.
- Written Consent:
  - Client must sign a release of information (ROI).

Levels of Consent

- Consent to use data within an agency for program or agency operations.

- Consent to share additional information across programs to coordinate case management and service delivery.

Privacy Summary

- Privacy refers to the safeguarding of protected personal information in the HMIS from open view, sharing or inappropriate use
- Protected Personal Information (PPI) is any information that might identify a specific individual or that might be manipulated or linked with other information to identify a specific individual

Baseline Privacy Standards

- Must comply with other federal, state, and local confidentiality law
- Must comply with limits to data collection (relevant, appropriate, lawful, specified in privacy notice)
- Must have written privacy policy - and post it on your web site
- Must post sign at intake or comparable location with general reasons for collection and reference to privacy policy
- May infer consent for uses in the posted sign and written privacy policy

Community Example: Akron, OH

- Coordinated Entry
- By-Name Veterans List
- Work Groups (e.g. HIV, RHY, Hoarding)

HMIS Role in Developing Data Sharing Systems

- Release of Information
- Policy Development (Security, Privacy, Reporting Incidents, Disaster Recovery)
- Annual Security Audits
- Vendor Inclusion
- Clearly-defined Roles and Responsibilities

HMIS Role in Developing Data Sharing Systems – Challenges and Successes

- Open Discussion
- What have been your challenges related to developing a data sharing system across multiple partners?
- What have been your successes related to developing a data sharing system across multiple partners?

Contact Information

Susan Starrett
Senior Program Manager, CSH
Susan.starrett@csh.org
302-530-7993

Joe Scalise
Vice President of Access Services, Info Line, Inc.
jscalise@infolineinc.org
330-315-0415