Protecting Data in an HMIS Environment: Privacy, Security, and Confidentiality Office Hours

October 2021

Brian Roccapriore (he/him), The Cloudburst Group
Mary Schwartz (she/her), Abt Associates

Expectations

- You should have seen / know the content of HMIS Governance 101
- This is an “Office Hours” presentation – we need to hear from you!

Agenda

- Introductions
- Review standards privacy & security AAQ response
- Review provisions and responsibility HMIS Privacy and Security Notice
- Live AAQ Session with Community Highlights

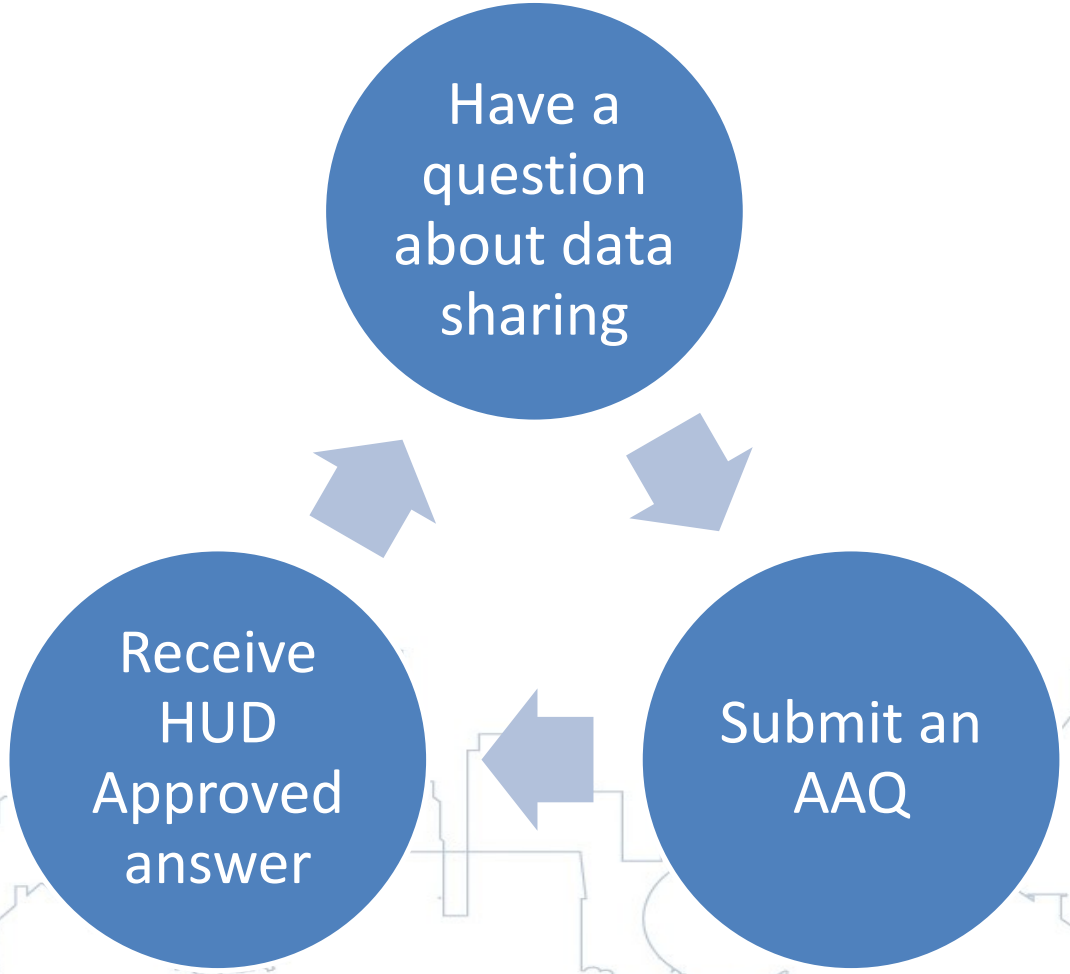
Learning Objectives

- Identify strategies to manage data in an HMIS environment that meet the needs of clients, projects, and the system while protecting and respecting client choice regarding how their personal information is managed
- Understand fundamentals of required and permitted uses and disclosures of clients' Personally Identifying Information (PII)
- Community Examples and Q&A

Poll!

- Have you submitted a privacy related AAQ?
  - Yes
  - No
  - What's an AAQ?

Privacy Policy Question Lifecycle



The “stock” HUD Approved Answer

Privacy Policy

The privacy and security standards, as described in the **2004 Data and Technical Standards Notice**, seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. Additionally, the **Coordinated Entry Management and Data Guide** offers the most recent guidance on Privacy in Chapter 2.

A provider must collect Personally Identifying Information (PII) by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. When a provider is required by law to collect information it must ask for the required information, although participants may refuse to provide the information and still receive services. In all circumstances, providers should make data collection transparent by providing participants with a written copy of the CoC’s Privacy Notice, describing the notice in plain language, and posting a public statement like the following:

We collect personal information directly from you for reasons that are discussed in our Privacy Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness. We only collect information that we consider to be appropriate.

Amending the Privacy Notice

Section 4.2.4 of the 2004 Notice discusses amendments to the privacy notice. A participating agency **must** state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the agency before the date of the change:

From the 2004 Notice: “An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A Covered Homeless Organization (CHO) must maintain permanent documentation of all privacy notice amendments.”

Updated guidance regarding data disclosures not requiring client consent

“Uses” are internal activities for which providers interact with participant PII. “Disclosures” of PII occur when providers share PII with an external entity.

Once collected, providers have obligations about how PII information may be used and disclosed. Uses and disclosures either are ***required*** by HUD (e.g., participants’ access to their own information, oversight of compliance with the HMIS data privacy and security standards) ***or are permitted*** by HUD (e.g., to provide services, reporting to funders). HUD’s required and permitted uses and disclosures must be stated in the CoC’s Privacy Notice.

HUD requires two mandatory disclosures regardless of their inclusion in the Privacy Notice:

Client access to their information; and

Disclosures for oversight of compliance with HMIS privacy and security standards.

HUD permits the following uses and disclosures of PII without participant consent, provided that the uses and disclosures are listed in the CoC’s Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, client consent is required:

To provide or coordinate services to an individual;

For functions related to payment or reimbursement for services;

To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; and

The “stock” HUD Approved Answer

For creating de-identified datasets from PII.

HUD also permits the following types of uses and disclosures of PII without participant consent, provided that these additional uses and disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, client consent is required:

Uses and disclosures to avert a serious threat to health or safety;

Uses and disclosures about victims of abuse, neglect or domestic violence;

Uses and disclosures for research purposes; and

Uses and disclosures for law enforcement purposes.

Method of Consent

Should consent need to be obtained from the client for uses and/or disclosures that are not listed on the Privacy Notice, the HMIS standards in effect at this time do not specify what method or terms of consent are appropriate in order to obtain client consent, nor do the current HMIS standards indicate that consent to share information about the members of a household must be obtained from all adult members of the household. Decisions about appropriate levels of consent may be made locally and in accordance with any local, state, or other federal privacy regulations applicable to the situation.

Authority to make changes in HMIS Policy and Data Ownership

Remember that the **CoC Program Interim Rule** gives CoCs authority over and responsibility for HMIS. As a result, data ownership/access questions should be addressed by the CoCs through any HMIS governance, policies, and/or agreements in place between associated parties.

More Assistance Needed

HUD understands that this updated guidance may change local policies and practices that have been implemented under older guidance.

If this updated guidance poses significant barriers to further HMIS implementation work, HUD recommends that you request HUD Technical Assistance (TA). If TA resources are available and your request is approved, a HUD TA provider can offer on-call or on-site TA depending on the complexity of the need. Submit your TA request through the **HUDExchange TA Portal**. Grantees should work in partnership with project sponsors to coordinate project sponsor TA requests.

You can find community examples of forms used for HMIS governance, privacy and consent purposes by visiting this website: **https://www.hudexchange.info/programs/coc/toolkit/responsibilities-and-duties/coordinated-entry-samples-toolkit/#data-management**

Please note: this response has been provided based on the current requirements and guidance available. Notices or other HUD-issued guidance in the future may change the current requirements. Additionally, the response provided in this email is specific to the question you submitted and may not apply to similar questions. Therefore, please use discretion in providing the response to others, as the answer may not apply to their particular situations.

Key Rules, Regulations, and Privacy Fundamentals

- **State and local privacy laws**
  - May place additional restrictions on sharing, using, or disclosing data
  - When privacy laws conflict, use the more restrictive law
- **HUD HMIS Data Technical Standards**
  - Establishes standards for collecting, using, and disclosing data in HMIS
- **Violence Against Women Act (VAWA), Family Violence Prevention Services Act (FVPSA), and Victims of Crime Act (VOCA)**
  - VAWA contains strong, legally codified confidentiality provisions that limit Victim Service Providers from sharing, disclosing, or revealing personally identifying information (PII) into shared databases like HMIS
- **Health Insurance Portability and Accountability Act (HIPAA)**
  - Governs how health care providers, health care clearinghouses, and health plans disclose data
- **42 CFR Part 2**
  - Restricts how drug and alcohol treatment programs disclose client records
- **Privacy Act (5 U.S.C. 552a)**
  - Applies to Federal Governments so is consulted at each policy revision

Amending the Privacy Notice

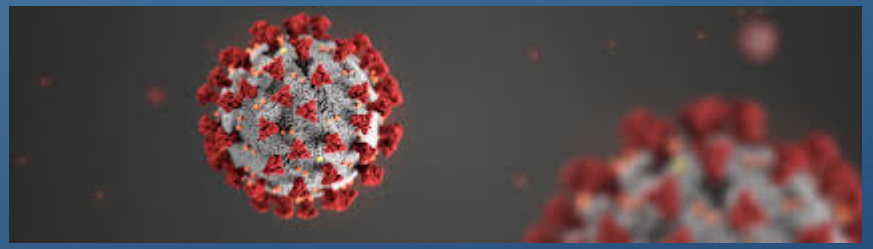
- You can and should amend the Privacy Notice if it doesn't include all allowable uses and disclosures
- Changes are retroactive as long as the Privacy Notice said they are; include this in any future version if it isn't already (it must be included)
- Go through CoC governing body to work through amendment approvals
- Maintain amendments on file at HMIS Lead

Data uses and disclosures not requiring client consent (if included in Privacy Notice)

- Mandatory regardless of inclusion in Privacy Notice:
  - Client access to information
  - Disclosures for oversight of compliance with security standards

- Uses and Disclosures Permitted if included in Privacy Notice:
  - To provide or coordinate services to an individual;
  - For functions related to payment or reimbursement for services;
  - To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions;
  - For creating de-identified datasets from PII;
  - Uses and disclosures to avert a serious threat to health or safety;
  - Uses and disclosures about victims of abuse, neglect or domestic violence;
  - Uses and disclosures for research purposes; and
  - Uses and disclosures for law enforcement purposes.

Case Study: Coronavirus



- Privacy Notice for CoC includes all allowable uses/disclosures from the AAQ
- Local public health authority wants a list of all shelter residents from HMIS to cross-reference with internal testing results
- Can the CoC provide the public health authority with all shelter data?

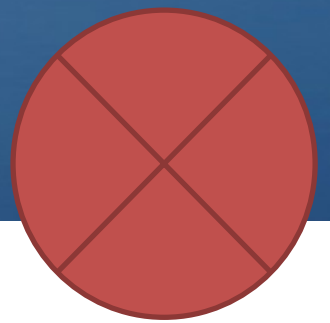
Yes

No

Method of Consent

- If a use or disclosure isn't included in the privacy notice, client consent is required; however,
  - 2004 notice does not specify what method of consent is required (inferred, written, verbal, etc.)
  - 2004 notice does not specify who can provide consent for members of the household
  - Decisions about appropriate levels of consent may be made locally and in accordance with any local, state, or other federal privacy regulations applicable to the situation

Case Studies: Unauthorized Disclosure



A. The HMIS Lead just included a screenshot with client PII when they submitted an HMIS AAQ regarding coordinated entry and EHV referrals.
B. Shelter A was accidentally given direct access to modify Shelter B data with administrative controls on the back-end. Reporting from each Shelter includes data from both, however no reports have been submitted yet.

Discussion:

- Which of these requires client notification?
- What is the remedy for each situation to ensure the least amount of damage to persons, organizations, and systems?
- Does your CoC have policies and procedures regarding data breaches, notifications, and remedies?

Authority to make changes in HMIS Policy and Data Ownership

- Remember that the CoC Program Interim Rule gives CoCs authority over and responsibility for HMIS. As a result, data ownership/access questions should be addressed by the CoCs through any HMIS governance, policies, and/or agreements in place between associated parties.

- Discussion:

1. Have any CoCs done this?
2. Does any CoC still have written Release of Information (ROI) requirements to enter and/or share HMIS data?
3. What are some initial steps to take to engage in this change work, should it be needed?

Data Uses and Disclosures

Once data is collected, providers have obligations about how that information is used and disclosed.

Uses are internal activities for which providers interact with client PII.

Disclosures of PII occur when providers share PII with an external entity.

Uses and disclosures are either:

- **Required** (e.g., providing a copy)
- **Permitted** (to provide services, reporting to funders, etc.), or
- **Prohibited** by other federal, state or local law (e.g. VAWA).

The provider's uses (internal) and disclosures (external) of collected information must be stated in the privacy notice.

Data Uses and Disclosures

HUD gives providers the authority for the following uses and disclosures without needing to obtain participant consent as long as they are clearly articulated in the Privacy Notice.

- Providing or coordinating services to an individual
- Creating de-identified client records from PII
- Carrying out administrative functions
  (e.g., legal, audit, personnel, oversight and management functions)
- Functions related to payment or reimbursement for services

Data Uses and Disclosures

Providers are also allowed (in some cases required) to disclose information in the following ways without participant consent, as long as they are clearly documented in the privacy notice.

- Uses and disclosures required by law
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures about victims of abuse, neglect or domestic violence
- Uses and disclosures for research purposes
- Uses and disclosures for law enforcement purposes.

Important: Uses and disclosures not listed in the privacy notice require the participant's consent.

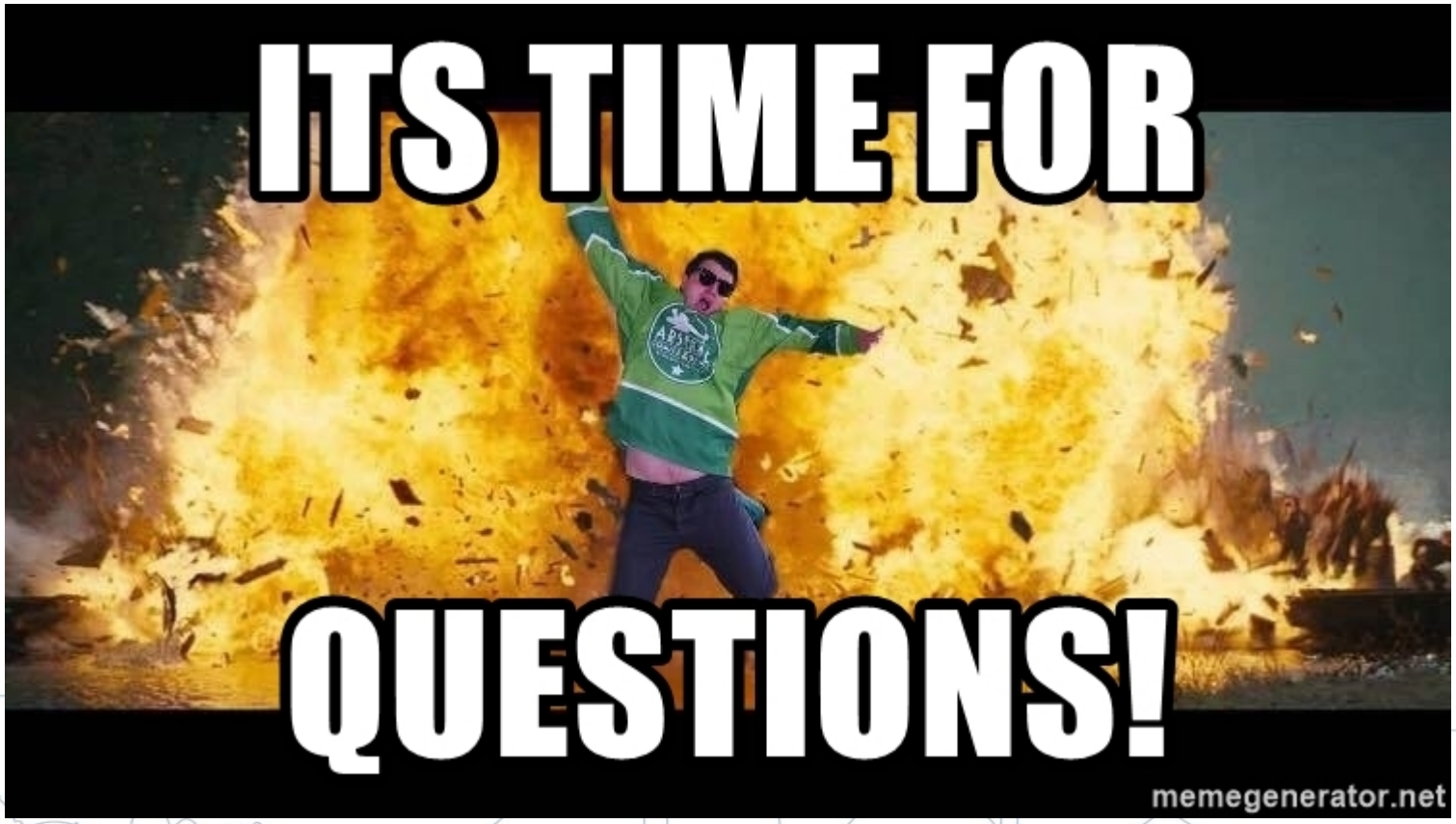
Implications for Victim Service Providers

- **Domestic violence providers are prohibited from entering PII into HMIS, and must use a comparable database**
  - This database must be comparable to HMIS in its capacity to support HUD privacy and security requirements and at a minimum, meet Data Standards requirements and produce HUD required reporting files.
- **Victims of domestic violence must have access to the coordinated entry process**
  - May be through a separate access point and assessment tool
  - Safety and confidentiality is essential when sharing data or referring clients
- Comparable Database Resources:
  - Comparable Database Manual
  - Comparable Database Vendor Checklist
  - Comparable Database Decision Tree
- Community Examples from Safe Housing Partnerships:
  - https://safehousingpartnerships.org/sites/default/files/2018-04/Coordinated%20Entry.pdf

More Assistance Needed…

- Submit an AAQ:
  - https://www.hudexchange.info/program-support/my-question/
- TA Requests:
  - https://www.hudexchange.info/technical-assistance/
- VAWA Support:
  - https://safehousingpartnerships.org/technical-assistance

Office Hours!



National Human Services Data Consortium

U.S. Department of Housing and Urban Development

Community Planning and Development

Key Takeaways/Next Steps

- **Recommended practices:**
  - ✓ Review / Update CoC Privacy Notice: CoC agencies must adopt this policy
  - ✓ Place a sign at data collection points explaining why information is being collected and how to obtain the CoC's privacy notice;
  - ✓ Include the participant's rights, the ways in which information may be used or disclosed (without written consent), a list of situations in which consent is required, the provider's responsibility to protect and secure participant information, and how the notice can be amended;
  - ✓ Be proactive and give the participant a copy of the privacy notice;
  - ✓ Have a legal advisor review privacy practices and determine how other local, state and federal laws impacts a provider's privacy and security requirements.

Thank you!

Brian Roccapriore (he/him)
Subject Matter Expert
The Cloudburst Group
brian.roccapriore@cloudburstgroup.com

Mary Schwartz (she/her)
Sr. Associate
Abt Associates
Collaborative Solutions
Mary_Schwartz@abtassoc.com

National Human Services Data Consortium