HMIS Privacy and Security Essentials

August 22nd, 2019

Agenda

1. Announcements and overview of webinar goals
2. Data privacy and security fundamentals
3. Why is privacy and security important for HMIS?
4. Responsibilities of HMIS Lead, Agencies and Users
5. 3-Step Privacy Process
6. Review of how to properly document MPA in Clarity
7. Common Errors in ROI Records
8. How to Document MPA Decline/ Revocation
9. Restricting Records for Clients who Decline/Revoke Authorization
10. Q & A

Data Privacy and Security

- **Data Privacy** - Legal requirements and information practices that regulate the collection, storage and use of personal information. Data privacy measures ensure that a person whose information is being used and disclosed by another party is informed and has choice in how their information is used.
- **Data Security** is the protection of personal protected information from unauthorized access, disclosure, use, or modification.

What is PPI or PII?

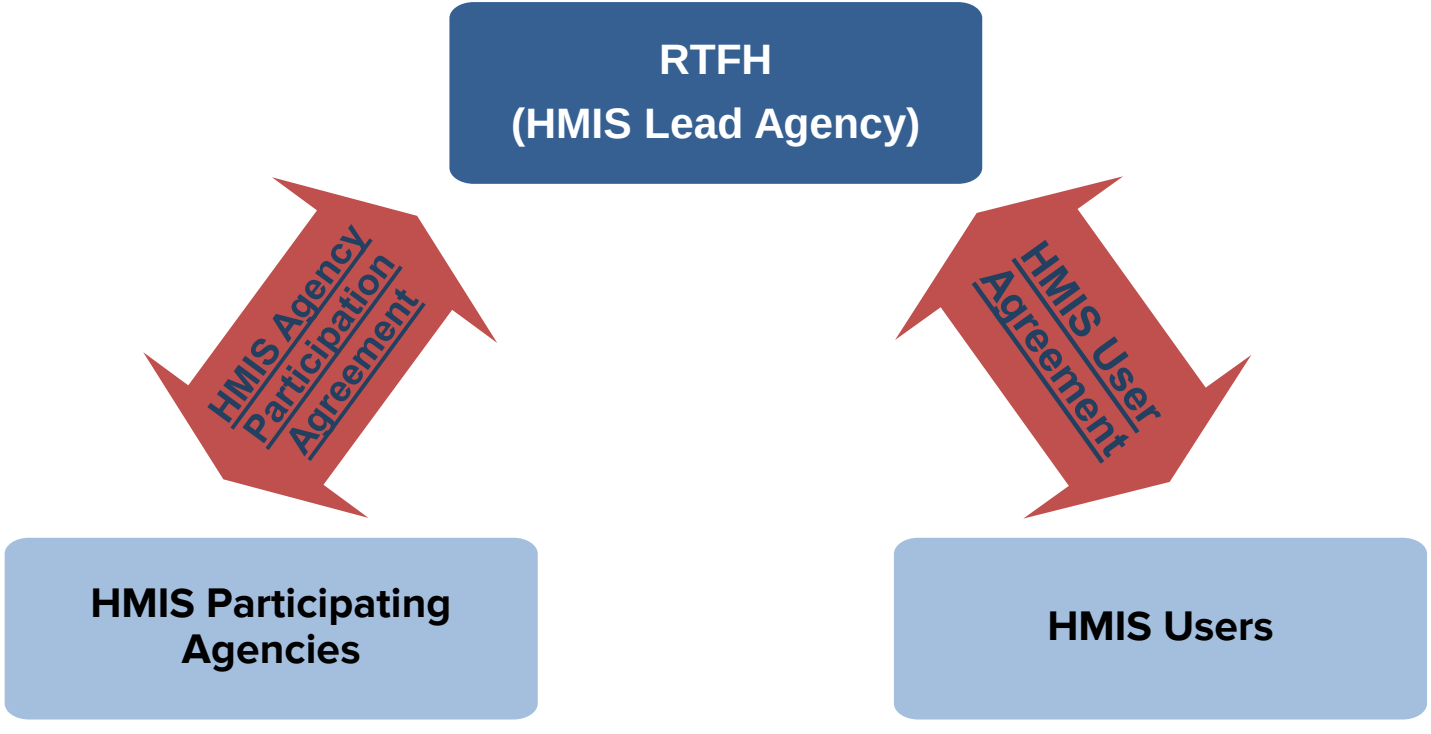
- PII: Personally Identifiable Information
- PPI: Personally Protected Information
- Definition of PPI from *HMIS Data and Technical Standards*:
  - *"Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that:*
    (1) Identifies, either directly or indirectly, a specific individual;
    (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or
    (3) can be linked with other available information to identify a specific individual."
- Examples of PPI:
  - First and last name
  - Date of Birth
  - SSN

Why is privacy and security important for HMIS?

- HUD's requirement that communities implement an HMIS system requires collecting, storing and handling PII/PPI.
- HMIS Data and Technical Standards lay out federal standards aiming to *"protect confidentiality…while allowing for reasonable, responsible and limited uses and disclosures of data".*
- Each Continuum of Care must assess requirements for its own HMIS implementation based on HUD's regulations and other applicable federal, state and local laws.
- San Diego's requirements are outlined in the HMIS Policies and Procedures and included appendices.

HMIS Policies and Procedures Flowchart

Participating Agencies and HMIS users both sign agreements formalizing their commitment to fulfill privacy, security and other requirements related to HMIS.



RTFH Responsibilities as HMIS Lead

- All system-wide policies and procedures.
- All privacy concerns related to HMIS.
- Monitoring in order to:
  - Detect and mitigate security risks
  - Identify and respond to security violations
  - Assess participating agencies compliance with HMIS Policies and Procedures
- Communicating requirements to agencies and providing technical assistance.
- Manage user licenses and access.

Participating Agency's Responsibilities

- Review and sign HMIS Agency Participation Agreement
- Review and ensure compliance with HMIS Policies and Procedures.
- Ensure compliance with HMIS procedures for collecting client data, including that staff comply with 3-Step Privacy Process.
- Report any suspected or real privacy or security incidents.
- Designate 4 key HMIS contacts and update them as-needed.
- Notify HMIS Lead Agency of personnel changes.
- Ensure users are trained and provide technical support.

HMIS Users' Responsibilities

- Review and sign HMIS User Agreement (upon first log-in to Clarity).
- Review and abide by all requirements in HMIS Policies and Procedures.
- Adhere to HMIS Ethics statement;
- Follow 3-step privacy process for HMIS data.
- Only enter and access data for the purposes of delivering and coordinating services.
- Maintain confidentiality of client data.
- Enter data accurately, based on client self-report and do not misrepresent information.
- Report observed security violations.

Security Reminders for All Users

- Only use your own username/password to log in.
- Always log out of HMIS when not using it.
- Be mindful of your physical space; if there is clear line-of-sight to your computer screen, consider a privacy screen.
- Use complex passwords; do not write your password down (and definitely don't write it down somewhere it can be accessed).
- DO NOT communicate PII via email or any other means – stick to Clarity unique identifier to refer to clients.
- Lock up any hard-copy HMIS records (inside locked file cabinet or office that is locked when not in use).
- Do not share HMIS data with organizations outside of the HMIS Trust Network.

3-Step Privacy Process

1. Mandatory Data Collection Notice
2. Notice of Privacy Practices
3. Multiparty Authorization (MPA)

Mandatory Data Collection Notice

- Click here to view notice on RTFH website.
- Must be posted at all client intake areas so that it's visible to clients before their information is collected and entered into HMIS.
- Informed consent:
  - Presence of poster informs clients that their information is being collected and stored in HMIS.
  - Also informs client they can review full privacy notice for more details if they request it.
- Not necessary to discuss notice with client unless they request more information.
  - If they request more information, do discuss it and provide NPP to fully inform them.
- Full-size poster should be posted at on-site spaces.
- Letter-size version of notice can printed from RTFH website and used in the field (for example, homeless outreach teams).

Notice of Privacy Practices (NPP)

- Click here to view NPP on RTFH website.
- NPP notifies client:
  - Why data is being collected, potential uses and disclosures
  - Their privacy rights around collected data
  - How to submit a grievance

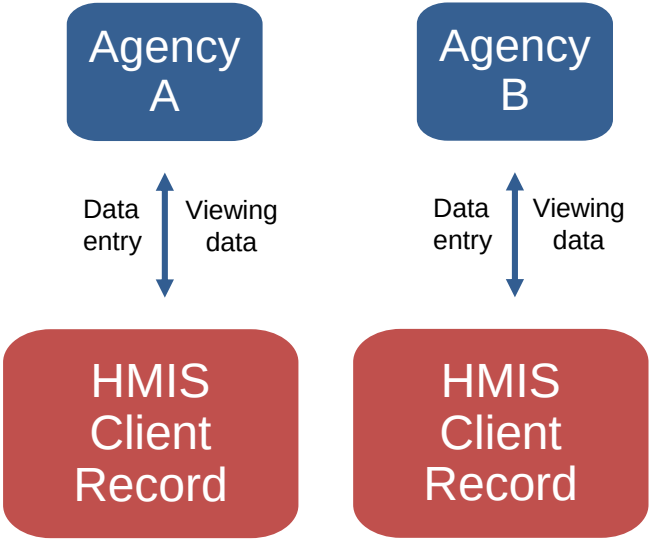
****CHANGES TO REQUIREMENTS FOR NPP****

- **No longer required to review by default with client.**
- **No longer required to obtain signature (form will be updated to remove signature area).**
- Still important to be familiar with information, ready to discuss and provide client copy upon their request.

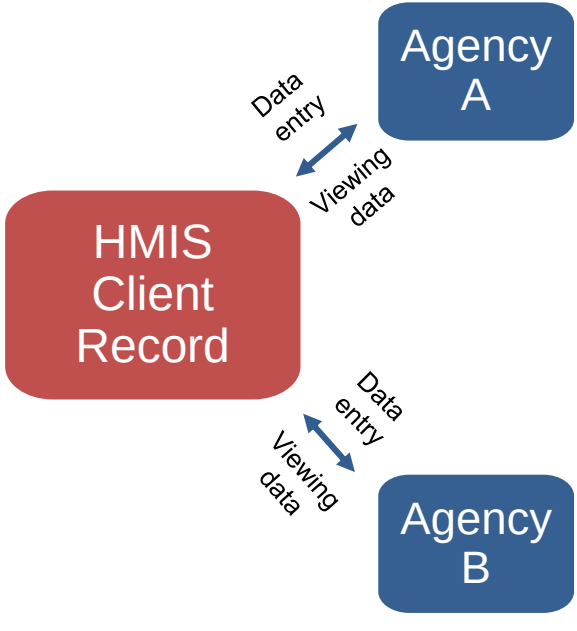
Data Collection vs. Data Sharing

Data collection and storage in HMIS involves agencies entering data into records and only their staff viewing that data. Data sharing in HMIS means that – in most cases – when an agency enters data all other CoC agencies using HMIS can see that data. For most agencies (except for a few exceptions), **all records they create in Clarity are shared by default**. This includes basic identifying and demographic information on the Client Profile, program enrollment data and other data entered in the client record.

Data Collection and Storage



Data Sharing



HMIS Trust Network

- Trust Network = All HMIS Participating Agencies that have signed a participation agreement.
- Trust Network providers share data via HMIS records.
- Benefits of sharing:
  - Helps in de-duplicating client records.
  - Improves providers' ability to coordinate services and provides comprehensive record of client needs/services.
  - Streamlines participation in CES process.
- Updated list of Trust Network providers available on RTFH website.
- List of providers on last two pages of MPA will be removed soon; clients can be referred to RTFH webpage with Trust Network list that is linked on MPA.

Multiparty Authorization (MPA)

- Click here to view MPA on RTFH website.
- San Diego City and County CoC's Release of Information form for HMIS.
- Informs the client what data is being collected and shared, informs them of their rights and includes a place to record their data sharing wishes: (1) their authorization to share data or (2) their decline to share data with any organizations.
  - If a client declines to share data, proper documentation of that decline includes client signature and checking checkbox labeled "I do not wish to share information with any organizations".
- Since San Diego's HMIS was opened/shared in Sept 2017, **this has been required to be discussed and a response collected for all clients**.
  - Not possible to create a new client record in Clarity without recording MPA response in the ROI area.
  - Outreach workers may not be able to discuss MPA with client easily during first several visits while building rapport. MPA should be discussed as early as possible in process, but outreach workers may create client record without MPA response if necessary. See instructions in Outreach cheat sheet for full details and contact support@rtfhsd.org with questions.
- MPA authorization is valid for 7 years.
- Clients who previously signed MPA can revoke consent to share data by completing Revocation form.
- Can a client sign the MPA for someone else? Only in 2 scenarios:
  - Parents can sign MPA for under-18 children.
  - Clients who require a legal guardian can have guardian sign for them.
- Check Clarity for an existing MPA before intake if you can! Once MPA is signed by client at any Trust Network provider, no need to ask client to sign again unless:
  - Their MPA will expire soon.
  - They declined previously and you are asking if they would now be willing to share.
- Client records were migrated from ServicePoint without MPA files so many clients do not have updated MPA records in Clarity. Review clients actively enrolled in your programs and update MPA's with either existing files you retained on-paper OR by collecting new signed MPA.

Documenting MPA in Clarity

- Release of Information Permission = “Yes” if client authorized to share.
- Start Date = Date of client signature.
- End Date = Defaults to 7 years from signature.
- Documentation Methods:
  - Electronic Signature – Can be used if it’s possible to have client sign using computer mouse or touchpad.
  - Attached PDF – Client signs paper copy of MPA which is scanned and uploaded.
  - Signed Paper Document – Only to be used in a temporary situation in order to create client record; must be updated within 24 hours.
  - Verbal Consent – Only valid for 2-1-1.
  - Household – only valid for:
    - Children under 18 whose parent signed an MPA for both themselves and child or
    - Client who requires legal guardian/conservator and that guardian signed for them.
    - MPA must be in parent/guardian’s Clarity record.

Common Errors in ROI Records

- Invalid documentation method = ***written consent required.***
- Date of signature on PDF file uploaded does not match ROI start date in Clarity.
- Permission = “No” for ROI but RTFH was not informed and client decline or revocation was not collected.
  - Only time when client would be created with a permission of “No” that is not due to client declining/revoking would be outreach worker creating client record without MPA because they have not yet been able to discuss it with client. In that case, ROI would be updated as soon as MPA is discussed.
- Review currently active clients in your programs for correct ROI records.
- RTFH monitoring visits will also include review of ROI data.

How to Document MPA Decline/ Revocation

- MPA Decline:
  - First time client discusses MPA, they decline to share data.
  - Client completes and signs paper MPA and checks “I do not wish to share information…” checkbox below signature line.
  - Not possible to document decline via Electronic Signature ROI option.
  - Scan and upload declined MPA into Files tab.
- Revocation of authorization:
  - Use if client has previously signed the MPA and is now revoking authorization to share data.
  - Not possible to document revocation via Electronic Signature ROI option.
  - Scan and upload Revocation into Files tab.
- Add ROI with Permission = “No”.
- If you are able to, you can set record to “Private” in ROI area.
- ALWAYS email support@rtfhsd.org to request assistance restricting client record. If you do not inform support, record may still be shared.
- If a client authorizes after previously declining, all previous data can be shared.
- See cheat sheet for com

Restricting Records for Clients who Decline/Revoke Authorization

Single-Agency Data History

- Contact Support@rtfhsd.org
- Only one agency has entered data into the Clarity record, so HMIS Support team can privatize record using Clarity's privacy feature.
- Data will be retained.
- Record will only be visible to users at the agency that created client record.

Multi-Agency Data History

- Contact support@rtfhsd.org.
- Multiple agencies have entered data into Clarity record, so it cannot be restricted automatically and has to be de-identified.
- Client profile will be scrubbed of all identifying details.
- Data in other areas (program enrollments, assessments, notes, files) must be privatized to agency that created data.
- Providers with active enrollments for client will be informed to retain unique identifier and PII on hard copy to be able to continue to update record.
- Any new data entered must be privatized to avoid sharing PII against client's wishes.