Alameda County Homeless Management Information System (HMIS)

Privacy and Security Procedures

Frequently Asked Questions

Consent

1. **Q: What is Informed Consent?**
   A: Being “informed” means having an understanding of the facts. If the client doesn’t understand the information provided, they can’t give informed consent allowing agencies that provide services to people who are homeless to access their personal identifying information.

2. **Q: What are the two consent models used in the Alameda County CoC? Do they both meet Informed Consent standards?**
   A: Alameda County uses the assumed consent and the explicit consent models. The assumed consent model involves a) posting a notice that explains the reasons for collecting HMIS information, and the uses and disclosures that are allowable; b) staff of covered homeless organizations discussing the contents of the notice with clients; and c) clients agreeing to provide personal information.

   Under the explicit consent model, clients sign a formal release of information (ROI) allowing service providers to share their personal information. Agency policy may require staff to secure signed ROIs. In addition, an ROI must be signed for a) any use or disclosure other than what is defined as allowable, and b) For any use or disclosure that is not listed in the CHO’s privacy notice.

   Both meet the Department of Housing and Development’s policy stated in the 2004 HMIS Data and Technical Standards.

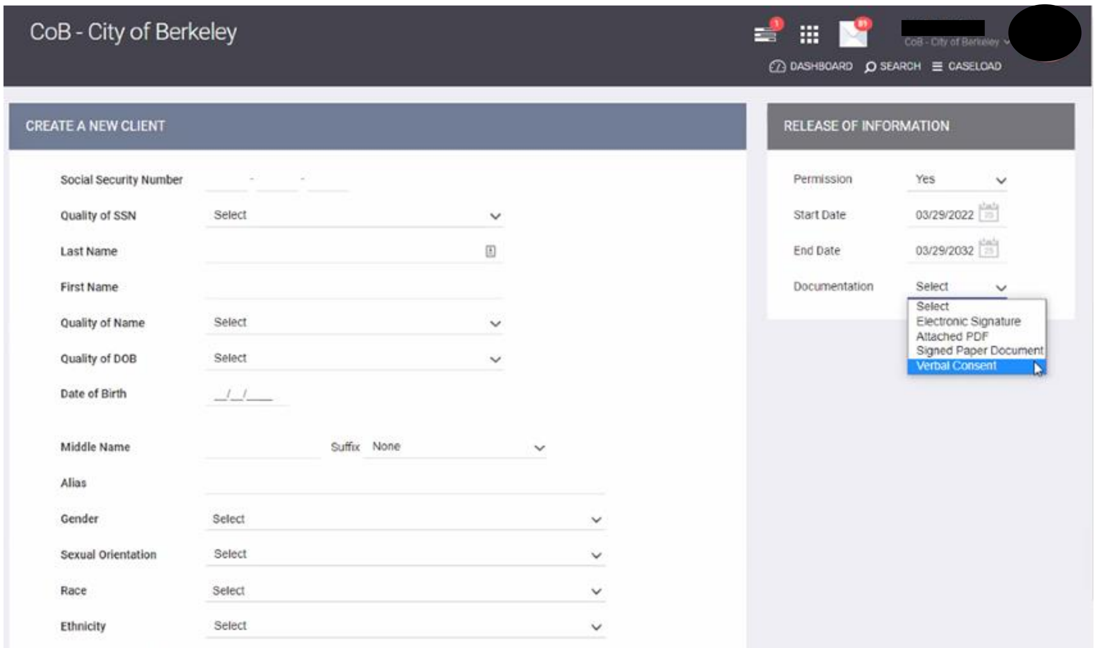
3. **Q: How will I know which consent model to use?**
   A: Your agency may specify which model you should use. If you are unsure, consult your agency’s HMIS Liaison.

4. **Q: What are the benefits of an assumed Consent model?**
   A: It is a low barrier approach to getting clients in the queue so their needs can be addressed in a timely, efficient and coordinated way.

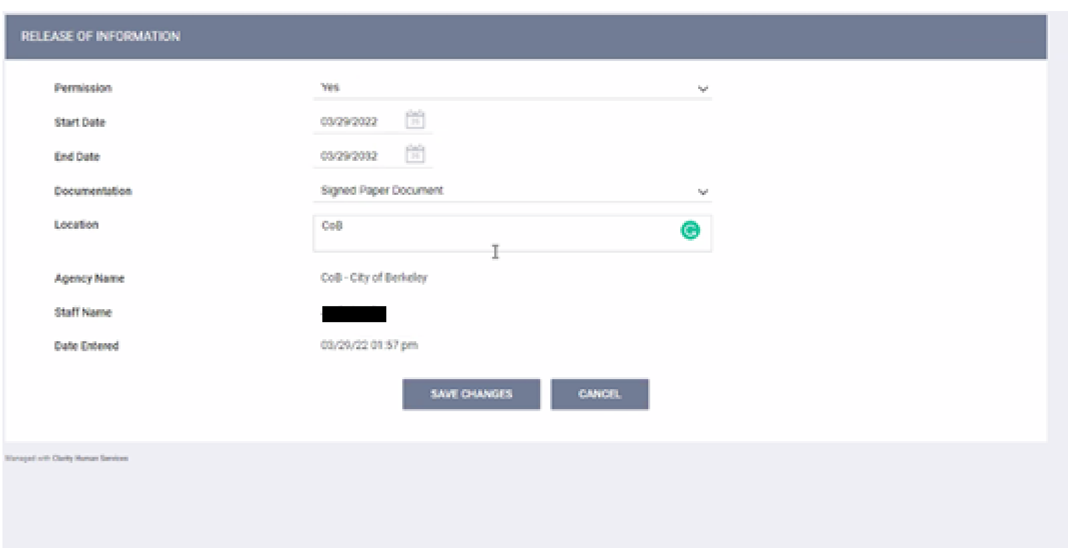
HMIS

1. **Q: How will Assumed Consent be recognized in the HMIS?**
   A: Service provider staff complete a Staff Attestation form indicating that they explain the Privacy Notice and the client has agreed verbally to share their personal information. Staff then record on the HMIS Release of Information screen that the client gave

permission to share their personal information and select “Signed Paper Document” as the type of documentation.(Assuming that there is another ROI popup box that would be discussed next.) B: If the client’s personal information is present in the HMIS and the ROI field indicates that an ROI has not been signed, then the client has given assumed consent.



- PII + Absence of an ROI = assumed consent
- Not necessary to upload attestation (value vs. burden); “Signed paper document” (below) means stored at City of Berkeley “



2. **Q: How will Explicit Consent be recognized in the HMIS?**
   A: The HMIS has a field for noting that a ROI has been signed. If the HMIS indicates that a client has an active ROI on file they have given explicit consent.

3. **Q: What if a client refuses, what forms do we need to complete?**

   A: If the client objects then the staff will check 'Yes' and then sign the document; no other forms need to be competed.

4. **Q: If a client is already enrolled in a program and we've completed the Staff Attestation form, but now we need to enroll the client in Coordinated Entry, do we need to do a new Staff Attestation form?**

   A: No need for a new Staff Attestation form, current form covers all HMIS programs.

5. **Q: What if a client isn't enrolling in a program at all, our only interaction with them is related to Coordinated Entry, do we do the Staff Attestation form then?**

   A: Yes, Coordinated Entry is a HMIS program and the Staff Attestation form is needed.

Training

1. **Q: What training is required before I can access the HMIS?**

   A: You must complete both the Privacy and Security course and the Software course to gain access to the HMIS. If you are processing personal information but not entering data into the HMIS, you only need to complete the Privacy and Security training.

2. **Q: How long does the training take?**

   A: The Privacy and Security course can be completed in one to two hours. Finishing the Software course takes four to six hours. This training is self-paced, so you can stop and restart the course whenever you want.

3. **Q: Do I need to repeat Privacy and Security training? How often?**

   A: The Privacy and Security training must be updated annually.

4. **Q: What if our staff completed the required compliance training offered by HCSA a few months ago. Do they still need to complete the Privacy and Security 2.0?**

   A: Per the Alameda county CoC and HMIS Lead MOU it is the obligation of CHO's to abide by the Privacy &Security Policy and in (24 CFR Parts 580.31). Also listed is the section from the policy and procedure around user training. This request will be brought to the HMIS oversight committee for further discussion and follow up with you on what has been decided.