
HMIS End User License Agreement (EULA)

Agency Name

Your Name

People with access to Multnomah County's Homeless Management Information System (HMIS), are referred to in this document as "End Users." All End Users are subject to the responsibilities specified below.

HMIS End User Roles & Responsibilities

1. Unless waived in writing by the County System Administrator (a designated staff member at your HMIS Lead Agency), End Users must provide a valid email address to the HMIS Lead Agency or Primary System Administrator for communication and End User profile setup purposes.
2. End Users will be familiar with and abide by all applicable federal, state and local data collection requirements, data standards, data completeness, accuracy and timeliness requirements, privacy and confidentiality rules and policies and procedures for HMIS.
3. Passwords
 - a. End Users will access HMIS only with their own unique username and password and keep this information private and secure.
 - b. End users must access and enter data into HMIS only using their own licensed account. End users will not allow another person to access HMIS using their account.
 - c. End Users will password protect all electronic files (e.g., .csv, .xls or .xlsx, .doc or .docx, etc.) containing personally identifying information ("PII") about Service Recipients. Files containing only the numeric client record number do not need to be password-protected.
 - d. End Users will not email passwords along with attached, password-protected files.
 - e. End Users will use strong passwords or passphrases for protection of files, devices and HMIS access.
 - f. End Users will not write passwords down or save passwords in internet browser auto-complete settings.
 - g. Should dual factor authentication become available for HMIS, End Users will use that in conjunction with strong passwords or passphrases.

- h. End Users will utilize password protected lock screens when stepping away from any device being used to access HMIS.
- 4. End Users will log in at least once every 30 days to maintain their account. The HMIS Lead will deactivate any accounts that have been inactive for 30 days or more.
- 5. End Users will store or dispose of all hardcopy and electronic records containing client information in a manner that protects clients privacy and confidentiality.
- 6. End Users will avoid storing personally identifying information of Service Recipients on their local computer drive.
- 7. End Users will avoid using client names, initials or other personally identifying information in emails whenever possible. This includes both the subject line and body of the email. Special circumstances may require the inclusion of names in emails. For example, names may be required when Coordinated Entry staff email landlords as part of the lease up process. Outside of such circumstances, avoid using names, initials or other PII in emails.
- 8. End Users will log out of HMIS when not actively using the system.
- 9. End User will not create test/sample records in the production site (i.e. the main HMIS that contains actual client data). End User will only create test records in the training instance of HMIS.
- 10. End Users will not input data for individuals when their relationship to the individual could create a conflict of interest (e.g., family members, friends, co-workers, etc.). End Users will notify their Agency Administrator if they believe a conflict of interest might exist.
- 11. End Users will only collect, enter, update and extract data that correspond to actual service provision of their Participating Agency within the approved area of service. End Users will never knowingly enter inaccurate data or alter accurate data. Verifiable third party documentation is recommended, where indicated, before updating existing data.
- 12. End Users will only access HMIS and the data therein, including client profiles, to successfully accomplish business operations that are relevant to their jobs. End Users will only access the minimum data necessary to accomplish authorized business purposes.
- 13. End Users will only access HMIS from Agency-approved devices.
- 14. End Users will not use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.
- 15. End Users will not use or otherwise manipulate HMIS in a manner intended to alter, harm, damage, or otherwise cause changes to the system that impair its functionality.
- 16. End Users will not enter profanity, offensive language or discriminatory comments based on any protected classification into HMIS. Protected classifications include but may not be limited to race, ethnicity, religion, national origin, ancestry, disabling condition, age, gender or sexual orientation.
- 17. End Users will only enter non-confidential information to the "Client Notes" section and comparable sections of the Client Profile.
- 18. End Users will report any unauthorized data access, use or disclosure, anomalous activity or non-compliant behavior with regard to HMIS to Agency Administrator, County System Administrator, Primary System Administrator and/or Comp Site System Administrator, as indicated.

19. End Users will proactively monitor and improve data quality, with a particular focus on data quality that is below data quality benchmarks, as specified by funder requirements and the CoC-specific Data Quality Plan.
20. End Users will follow data entry timeliness requirements, as set forth by their community's HMIS Lead Agency.
21. End Users will coordinate and comply with instructions from Agency Administrator, HMIS Lead Agency and/or Primary System Administrator to regularly monitor and improve data quality, specifically with regard to data completeness, accuracy and timeliness.
22. End Users will coordinate and collaborate with their designated Agency Administrator(s) and/or HMIS Lead Agency for technical assistance as needed.
23. End Users will explain any information in their agency's privacy notice that a service recipient does not understand. End Users will provide a copy of its privacy notice to any service recipient upon request.
24. Unless otherwise allowed by the *Privacy & Security Notice* and the community HMIS Policies & Procedures, End Users will receive informed consent from service recipients, their parent or those authorized to sign on their behalf, as documented in a Release of Information form, prior to disclosing any HMIS data or enabling HMIS data sharing to End Users in other agencies.
25. End Users will notify their Agency Administrator and/or HMIS Lead Agency if they leave the position that authorizes their access to HMIS.

I affirm the following:

1. I have read, understand and will abide by the terms of this document.
2. I have read, understand and will abide by the terms of my community's HMIS Policies & Procedures document.
3. I have read, understand and will abide by my Agency's Privacy Notice.
4. I acknowledge that noncompliance with the above roles & responsibilities may be grounds for suspension or termination of my employment and/or HMIS access.
5. I acknowledge that the terms of this agreement will survive the termination of my employment with the Agency identified above.
6. I acknowledge that future versions of this agreement will supersede this agreement.
7. I acknowledge that this agreement may be renewed periodically based upon the needs of the HMIS Lead Agency or the Primary System Administrator.

Signature, HMIS End User

Date of Signature

HMIS End User Title

HMIS End User Email

This agreement should be kept on file at the Agency and shared with the HMIS Lead Agency or Primary System Administrator upon request. Forms for individuals no longer employed by the Agency should be kept on file for seven years following the date of termination. The Primary System Administrator or HMIS Lead Agency may monitor compliance at any time.

Revision History

August '26

- Replaced references to “Community Services Software” or “CSS” with “Homeless Management Information System” or “HMIS”, respectively.
- Added the following policies:
 - End User will not create test/sample records in the production site (i.e. the main HMIS that contains actual client data). End User will only create test records in the training instance of HMIS.
 - End users must access and enter data into HMIS only using their own licensed account. End users will not allow another person to access HMIS using their account.
 - End Users will avoid using client names, initials or other personally identifying information in emails whenever possible. Special circumstances may require the inclusion of names in emails. For example, names may be required when Coordinated Entry staff email landlords as part of the lease up process. Outside of such circumstances, avoid using names, initials or other PII in emails.
 - End Users will log in at least once every 30 days to maintain their account. The HMIS Lead will deactivate any accounts that have been inactive for 30 days or more.
 - End Users will not input data for individuals when their relationship to the individual could create a conflict of interest (e.g., family members, friends, co-workers, etc.). End Users will notify their Agency Administrator if they believe a conflict of interest might exist.