VIA LINK

LISTENING • UNDERSTANDING • CONNECTING

HMIS ACCOUNT REQUEST AND ACCESS STATEMENT

All users must complete this form to get access to the LSNDC Homeless Management Information System (HMIS).

Completing this form authorizes VIA LINK, the REGIONAL LSNDC LEAD AGENCY, to give you a unique HMIS login and password. This will allow you to view, add, edit, delete, and potentially share your agency's client data in the LSNDC database.

By law, you are **NOT allowed to share** your login and password with anyone else. Sharing your login information is a serious violation and could result in you being permanently banned from the LSNDC system.

If you have any questions about this form, please contact your Regional LSNDC System Administrator at 504-896-2010.

REQUEST FOR A LSNDC SERVICEPOINT USER ACCOUNT

Account is for the following paid employee/student intern:

Employee's E-mail:	**Employee's Phone Number:**
Employee's Title:	**Immediate Supervisor's Name**

AUTHORIZE EMPLOYEE'S ACCESS TO CLIENT RECORD

Name of your agency's program(s) that this user can access, allowing for them to add, edit, and delete client data:

- ○ User has professional license for and is authorized to document ICD-9 codes in client files. (Additional costs related to ICD-9 code access may apply.)
- ○ User has professional license for and is authorized to document CPT codes in client files. (Additional costs related to CPT code access may apply.)
- ○ User has professional license for and is authorized to document DSM-IV-TR codes in client files. (Additional costs related to DSM-IV-TR code access may apply.)
- ○ Allow user to change the security settings of client records. This feature lets the user "open" and "close" portions of current client data to other agencies.
- ○ Allow User to "Back-Date" Releases of Information. This feature lets the user share past or "Back-Dated" client data with other agencies.

Executive Director's Signature (Date):

Regional LSNDC System Administrator (VIA LINK) Signature (Date):

Helen Meridy 9/2/2025

HMIS SUPPORT PORTAL https://vialinkhmis.org/support-portal/

VIA LINK
LISTENING • UNDERSTANDING • CONNECTING

HMIS User Policy, Code of Ethics, User Statement of Confidentiality & Responsibility Statement

USER POLICY

It is a client's decision about which information, if any, is entered into HMIS and whether that information is to be shared with any other HMIS Partner. The Client Consent Form and Client Authorization for Use/Disclosure of Protected Information must be signed by Client before any identifiable Client information is designated in HMIS for sharing with any Partner Agencies. User shall insure that prior to obtaining Client's signature; the Client Authorization for Use/Disclosure of Protected Information was fully reviewed with Client in a manner to insure that Client fully understood the information (e.g. securing a translator if necessary).

USER CODE OF ETHICS

- Users must be prepared to answer Client questions regarding HMIS.
- Users must faithfully respect Client preferences with regard to the entry and sharing of Client information within HMIS.
- Users must accurately record Client's preferences by making the proper designations as to sharing of Client information and/or any restrictions on the sharing of Client information.
- Users must allow Client to change his or her information sharing preferences at the Client's request.
- Users must not decline services to a Client or potential Client if that person refuses to allow entry of information into HMIS or to share their personal information with other agencies via HMIS.
- The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.
- Users will not solicit from or enter information about Clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.
- Users will not use HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity.
- Upon Client written request, users must allow a Client to inspect and obtain a copy of the Client's own information maintained within HMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client.
- Users must permit Clients to file a written complaint regarding the use or treatment of their information within HMIS. Client may file a written complaint. Clients may not be retaliated against for filing a complaint.

Statement of Confidentiality

I agree to maintain strict confidentiality of information obtained through HMIS. This information will be used only for the legitimate client service and administration of the above named Agency. Any breach of confidentiality will result in my immediate termination of participation in the HMIS.

I understand and agree to comply with all the statements listed above.

HMIS User Signature, HMIS User Name (please print), Date

Helen Meridy 9/2/2025

HMIS Director's Signature, Date

VIA LINK
LISTENING • UNDERSTANDING • CONNECTING

HMIS User Policy, Code of Ethics, User Statement of Confidentiality & Responsibility Statement

USER RESPONSIBILITY

Your User ID and Password give you access and authority to use the HMIS System. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination of User privileges.

- My User ID and Passwords must be physically secure and not to be shared with anyone, including other staff members, supervisors or Executive Director.
- I understand that the only individuals who can view information in HMIS are authorized users and the Client to whom the information pertains.
- I understand that my access to HMIS is limited to my designated work and this location must meet all HMIS Data and Technical Standards.
- I may only view, obtain, disclose, or use client data from HMIS that is necessary to perform my job and that these rules apply to all users of HMIS, whatever their work role, position, or location.
- Clients have the right to see their information on HMIS. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.
- I understand that failure to log off HMIS appropriately may result in a breach in client confidentiality and system security. If I am logged into HMIS and must leave the work area where the computer is located, I must log-off of the HMIS before leaving the work area.
- A computer that has HMIS “open and running” shall never be arranged so that unauthorized individuals may see the information on the screen.
- Hard copies and downloads of information from the HMIS onto a hard drive or disk must be kept secure to ensure that only appropriate agency staff has access.
- When hard copies and downloads of HMIS Client information are no longer needed, they must be properly destroyed as described in your agency’s privacy and confidentiality policies.
- I understand that I must not change the closed security on any Client data unless the Client has given informed consent, through a signed Client Consent Form and Client Authorization for Use/Disclosure of Protected Information. The HMIS Security settings must always reflect the Client’s expressed wishes as documented through the Informed Consent process.
- I understand that in the event that I am terminated or leave my employment with this agency my access is revoked, and I must not use my User ID and Passwords to access to the HMIS.
- If I notice or suspect a security breach, I must immediately notify the HMIS System Administrator.

I understand and agree to comply with all the statements listed above.

HMIS User Signature, HMIS User Name (please print), Date

Helen Meridy 9/2/2025

HMIS Director’s Signature, Date

LSDNC USER AGREEMENT

VIA LINK
LISTENING • UNDERSTANDING • CONNECTING

USER RESPONSIBILITY STATEMENT:

Your User ID and Password gives you access and authority to use the LSNDC System. Initial each item below to indicate your understanding and acceptance of the user responsibilities and the proper use of your User ID and Password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination of User privileges.

- I understood I am required to sign an acknowledgement that I have read and understood the LSNDC Standard Operating Procedures.
- I understand my User ID and Passwords must be physically secure and not to be shared with anyone, including other staff members, supervisors or Executive Director.
- I understand that the only individuals who can view information in the LSNDC System are authorized users and the Client to whom the information pertains.
- I understand that my access to the LSNDC System is limited to my designated work and this location must meet all HUD HMIS Data and Technical Standards.
- I understand I may only view, obtain, disclose, or use client data from the LSNDC System that is necessary to perform my job and that these rules apply to all users of the LSNDC System, whatever their work role, position, or location.
- I understand clients have the right to see their information in the LSNDC System. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.
- I understand that failure to log off the LSNDC System appropriately may result in a breach in client confidentiality and system security. If I am logged into HMIS and must leave the work area where the computer is located, I must log-off of the LSNDC System before leaving the work area.
- I understand a computer that has the LSNDC System "open and running" shall never be arranged so that unauthorized individuals may see the information on the screen.
- I understand hard copies and download of information from the LSNDC System onto a hard drive or disk must be kept secure to ensure that only appropriate agency staff has access.
- I understand what is described in the LSNDC Standard Operating Procedures. When hard copies and downloads of the LSNDC System Client information are no longer needed, they must be properly destroyed.
- I understand that I must not change the closed security on any Client's signed LSNDC Client Release of Information. The LSNDC System security settings must always reflect the Client's expressed wishes as documented through the LSNDC Client Release of Information.
- I understand that if I am no longer employed with this agency my access is revoked immediately, and I must not use my User ID and Passwords to access to the LSNDC System.
- I understand if I notice or suspect a security breach, I must immediately notify the Regional System Administrator at Clifton Harris at 504-899-6519.

I understand and agree to comply with all the statements listed above

Executive Director's Signature (Date): ____

User Signature (Date): ____

LSDNC USER AGREEMENT

VIA LINK
LISTENING • UNDERSTANDING • CONNECTING

USER POLICY:
It is a Client's decision about which information is to be shared with any other Louisiana Services Network Data Consortium (LSNDC) Partner Agency. The LSNDC Client Release of Information must be signed by Client before any Client information is designated in LSNDC System for sharing with any Partner Agencies. User shall ensure that prior to obtaining Client's signature the LSNDC Client Release of Information was fully reviewed with Client in a manner to ensure that Client fully understood the information (e.g. securing a translator if necessary).

USER CODE OF ETHICS
Users must not decline services to a Client or potential Client if that person refuses to allow entry of information into the LSNDC System or to share their personal information with other agencies via the LSNDC System.

Users must be prepared to answer Client questions regarding the LSNDC System.

Users must faithfully respect and accurately record Client preferences with regard to the entry and sharing Client information within the LSNDC System.

Users must allow Client to change his or her information sharing preferences at the Client's written request.

The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.

Users will not solicit from or enter information about Clients into the LSNDC System unless the information is required for a legitimate business purpose such as to provide services to the Client.

Users will not use the LSNDC System for any violation of any law, to defraud any entity or conduct any illegal activity.

Upon Client written request, users must allow a Client to inspect and obtain a copy of the Client's own information maintained within the LSNDC System. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client. For example, client doesn't have the right to see client-related information that has specifically been gathered from the LSNDC system in preparation for a court case involving Client. This would not include the kind of client data typically entered into the LSNDC system but only information relevant to the action or proceeding mentioned.

Users must permit Clients to file a written complaint regarding the use or treatment of their information within the LSNDC System. Client may file a written complaint using the LSNDC Client Grievance Form and send it to Regional System Administrator: VIA LINK, 5001 Hwy 190, Suite C-1, Covington, LA 70433. Clients may not be retaliated against for filing a complaint.

CONFIDENTIALITY STATEMENT: I agree to maintain strict confidentiality of information obtained through the LSNDC System. This information will be used only for the legitimate client service and administration of the above-named Agency. Any breach of confidentiality will result in my immediate termination of participation in the LSNDC System.

I understand and agree to comply with all the statements listed above.

Executive Director's Signature (Date): ______________________________

User Signature (Date): ______________________________________