Lake County Coalition for the Homeless

Lake County HMIS Policies and Procedures Manual

Approved by LCCH Board, August 29, 2019

Contents

Section 1: Introduction

The ServicePoint® Project in Lake County, Illinois is guided by the following vision:

> Every human service consumer in Lake County has access to effective, comprehensive services and care that will help them enhance their lives.

While ServicePoint® serves as the Homeless Management Information System (HMIS) for the Waukegan/ North Chicago/Lake County Continuum of Care (IL-502). The ServicePoint® Project has encompassed goals greater than HMIS requirements. The project is an effort of the Lake County Coalition for the Homeless under the leadership of Lake County Community Development. These groups have come together to see the realization of the project's vision (above) and to make progress toward the project goals to:

1. Increase agency collaboration
2. Reduce barriers to service for clients
3. Measure system performance

ServicePoint® was originally chosen and designed as Lake County's Homeless Management Information System (HMIS) in 1999. All homeless services providers who receive funding through the U.S. Department of Housing and Urban Development (HUD)'s Continuum of Care (CoC) and Emergency Solutions Grant (ESG) programs are required to utilize HMIS.

The current uses of ServicePoint include:

- HMIS – Homeless Management Information System
- Coordinated Entry – Process by which people in need of housing are evaluated and directed to the most appropriate service provider as capacity permits.
- Referral Network – System used by various service agencies to alert one another to a client's need for additional service.
- Find Help Lake County – On-line directory of Services available in Lake County

The ServicePoint Coordinating Council's policy manual governs all use types. This set of policies will govern two use types: Homeless Management Information System and Coordinated Entry. All agencies must comply with both sets of policies. There will be no contradictions between the sets of policies.

Governing Values

The following values are considered foundational to the HMIS System. These values will be reflected in all policies and procedures.

Ethical and Legal Use of the System and Treatment of Client Data

Use of HMIS will not impede or reduce services to clients. The policy decisions for how HMIS is used will seek to not do any harm to clients. The HMIS policies are designed to comply with all laws regarding client rights related to privacy and security of their information. The policies protect against the recording of information in unauthorized locations or systems. Only staff that work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, or edit client records. Additional privacy protection policies include:

a) No client records will be shared electronically with another agency without written client consent;
b) Client has the right to not answer any question (refusals may hinder access to care depending on individual program requirements);
c) Client-identifying information is stored in encrypted form at the central server;
d) Client has the right to know who has added to, deleted, or edited their client record;
e) Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection.

Data Integrity and Standardization

The value of HMIS is increased when there is standardization in implementation. Therefore, whenever feasible, the policies and use of HMIS will seek to standardize provider configuration, data standards and training. Data are the most valuable assets of the Lake County HMIS. It is our policy to protect this asset from accidental or intentional unauthorized modification, disclosure, or destruction. Our data security program must be a well-organized and cost-effective plan, which formulates the safeguards to protect client, agency, and policy level interests. Lake County staff is responsible for controlling access to the system and will use three access controls to carry out this responsibility: user authentication, Public Key Infrastructure and Secure Socket Layer (SSL).

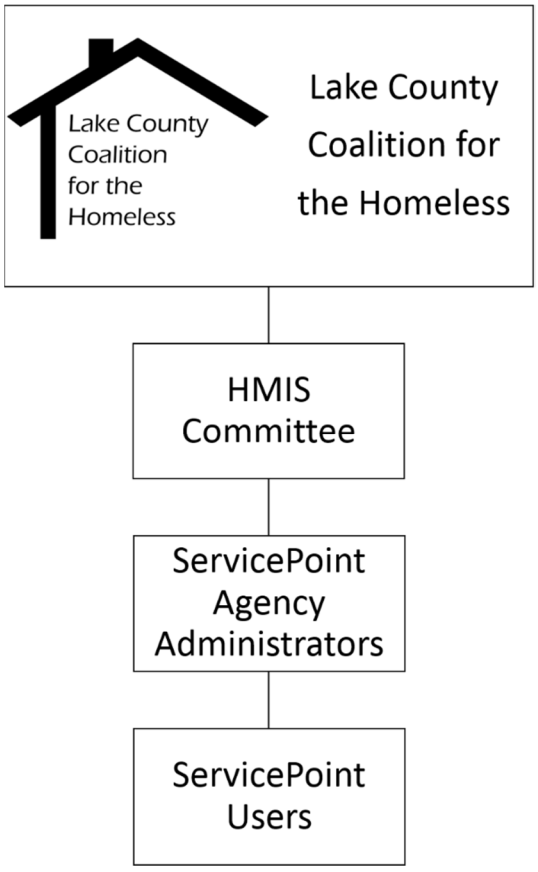
Compliance with HUD's HMIS regulations

There is a foundation and priority given to policies and procedures required by HUD for compliance as a Homeless Management Information System. Policies will support the maximization of points on the Continuum of Care funding application.

Roles and Responsibilities

The HMIS System is managed and utilized by individuals in a variety of roles that include:

- Board of Directors (Lake County Coalition for the Homeless)
- WellSky Housing & Community Services
- ServicePoint® System Administrator
- ServicePoint® Coordinating Council
- HMIS Committee
- Agency Accountability Officer
- Agency Administrators
- Users



Roles and Responsibilities for each of these groups follow:

Board of Directors (Lake County Coalition for the Homeless)

- Approve HMIS development strategies as recommended by the System Administrator and the HMIS Committee
- Assign individuals to HMIS Committee as needed

WellSky Housing & Community Services

- Maintenance and monitoring of database functionality, speed, security, and backup
- Maintenance of database server and hosting environment
- Administration of internal and external networking components
- Administration of web servers and firewalls
- Informing the System Administrator of any outages

ServicePoint® System Administrators

- Provide training and technical assistance to participating agency administrators on all policies and procedures related to HMIS including agency/provider setup, user questions, network questions, system functionality, and reporting
- Monitor access to HMIS by users and audit usage
- Schedule and facilitate HMIS Committee and Agency Administrator meetings.
- Assure compliance with applicable HUD and other grants and federal regulations
- Deactivate user accounts after 7 months of inactivity
- Manage contracts with and serve as liaison to WellSky Housing & Community Services
- Build and maintain assessments that will correctly obtain required data elements and agency-specific data elements
- Monitor completeness and integrity of data collected and data collection practices
- Coordinate implementation of upgrades and future releases/upgrades
- Provide support needed to ensure timely submittal of reports required for any participating agency
- Communicate system availability, training site availability, planned outages, and other pertinent Lake County information to Agency Administrators
- Creating technical documentation on the use of Lake County's customized HMIS system
- Ensure compliance with HMIS policies, including minimum data elements required, meeting participation, and privacy protection provisions
- Develop standardized core user training materials and conduct regular trainings

ServicePoint® Coordinating Council

- Guide the implementation of ServicePoint® county-wide
- Develop, inform, and review ServicePoint® policies and procedures including roles & responsibilities, confidentiality & informed consent, release of information, privacy practices, and the user code of ethics
- Select minimal data elements to be collected by all programs participating in ServicePoint® with consideration for the needs of all use types
- Reviewing policies and procedures that have an impact across use-types.
- Developing guidelines for how data sharing is handled

HMIS Committee

- Guide the HMIS implementation county-wide
- Develop, inform, and review HMIS policies and procedures
- Select minimal data elements to be collected by all programs participating in HMIS
- Develop strategies that ensure that all homeless service providers are entering information into HMIS to ensure full coverage of homeless service providers.

Agency Accountability Officer

- Assume responsibility for integrity and protection of client-level data entered into the HMIS system
- Maintain an active Partnership Agreement with Lake County customized to the participating agency's implementation preferences
- Assign at least one Agency Administrator
- Establish business controls and practices to ensure organizational adherence to the HMIS policy and procedures for Lake County
- Resolve issues relating to agency participation in meetings, data integrity, etc.

Agency Administrators

- Serve as the primary point of contact and support for the ServicePoint® System Administrator
- Maintain provider profiles for agency and programs and ensure up-to-date information in FindHelpLakeCounty.org
- Ensure the completeness, accuracy, and protection of all data entered into HMIS for the agency
- Determine appropriate workflows and procedures for customized HMIS use
- Create quick lists, reports, and other agency-specific requirements
- Configure visibility settings
- Create usernames and passwords for appropriate agency users
- Deactivate user accounts when access is no longer required
- Conduct new user orientation including checklist and User Policy, Responsibility Statement, and Code of Ethics
- Train agency users on the proper use of HMIS including a review of Policies and Procedures and any agency policies that impact the security and integrity of client information
- Notify agency users of any interruptions in service
- Ensure agency representation is present for at least 60% of relevant Agency Administrator meetings per year and relay relevant information to his/her agency
- Monitor completeness and integrity of data entered in HMIS
- Monitor user adherence to policies and procedures and agency-specific procedures
- Provide first-tier technical support for users
- Administer agency-specified business and data protection controls
- Detect and respond to violations of the Lake County HMIS Policy and Procedures or agency procedures
- Maintain a file of signed User Policy, Responsibility Statement, and Code of Ethics documents

Users

- Sign User Policy, Responsibility Statement, and Code of Ethics
- Complete system-wide new user training
- Enter data accurately and in a timely fashion
- Comply with relevant policies and procedures
- Inform clients about the agency's use of HMIS
- Solicit client consent before entering client data into HMIS
- Solicit a Release of Information (when appropriate) before disclosing or unlocking client information to other programs/agencies.
- Take responsibility for the security of their usernames and passwords and any actions undertaken with their username and password
- Report concerns about HMIS usage, security, etc. to their Agency Administrator

In addition to the responsibilities listed above all HMIS stakeholders and users must comply with applicable state and federal laws.

Section 2: Data Quality Plan

HMIS Participation Requirements

Mandatory Participation

All programs that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services must meet the minimum HMIS participation standards as defined in this policy. These participating agencies will be required to comply with all applicable operating procedures and must agree to execute and comply with a ServicePoint® Data Services Agreement.

Voluntary Participation

While HUD does not require providers that do not receive HUD funds to participate in HMIS, the Lake County Coalition for the Homeless works closely with non-funded agencies to articulate the benefits of the HMIS and strongly encourages their participation in order to achieve a comprehensive and accurate understanding of homelessness and other social service needs in Lake County. These participating agencies will also be required to comply with all applicable operating procedures and must agree to execute and comply with a ServicePoint® Data Services Agreement.

Hardware, Connectivity, and Computer Security Requirements

Internet Connectivity

Partner Agencies must have Internet connectivity for each workstation accessing HMIS. To optimize performance, all agencies are encouraged to secure a high-speed Internet connection with a cable modem, DSL, or T1 line. Agencies expecting a very low volume of data may be able to connect using a dial-up connection; however, satisfactory performance is not guaranteed with this option.

Security Hardware/Software

All workstations accessing HMIS need to be protected by a securely configured firewall. If the workstations are part of an agency computer network, the firewall may be installed at a point between the network and the Internet or other systems rather than at each workstation. Each workstation or mobile computing device also needs to have anti-virus and anti-malware programs in use and properly maintained with automatic installation of all critical software updates.

Participation Requirements

Identification of Agency Administrator

Designation of one or more key staff persons to serve as Agency Administrators.

Training

Commitment of Agency Administrator and designated staff persons to attend training(s) prior to accessing the system online. Note: Staff will NOT be allowed to attend training until the ServicePoint® Data Services Agreement is signed by the agency's Executive Director (or designee).

Client Consent Forms

Authorization to Share Information Using ServicePoint® form must be utilized by the Participating Agency to authorize the sharing of clients' personal information electronically with other Participating Agencies through HMIS where applicable. (See attached Authorization to Share Information Using ServicePoint® form)

Data Standards

Agency staff shall collect the universal and program specific data elements as defined by HUD and other data elements as determined by the HMIS Committee for all clients served by programs participating in HMIS. Additional data elements may be collected at the discretion of the Participating Agency/Program. Data may be shared with other agencies subject to appropriate consent and network data sharing agreements. (See attached Minimum Data Standards)

Fees

Agency will be responsible for fees associated with usage of HMIS. These include new user setup fees, annual user licenses, and annual reporting licenses. Agency will be invoiced by Lake County on an annual basis. (See attached Fee Schedule) If an agency fails to pay for setup fees and/or annual user licenses, this agency's ServicePoint® Data Services Agreement may be terminated.

Participation Agreements

Agency is required to sign the ServicePoint® Data Services Agreement stating their commitment to comply with the policies and procedures for effective use of the system and proper collaboration with Lake County HMIS staff. (See attached Agreement) Agency must also participate in annual re-certification of and training on ServicePoint® policies and procedures.

Auditing

Agency may be subject to audits by the ServicePoint® System Administrator to verify compliance with ServicePoint® policies and procedures.

Fee Schedule

Fee Schedule for Homeless Programs

All programs that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services will adhere the fee schedule below. This includes, but is not limited to, programs funded through the Continuum of Care, Supportive Services for Veterans Families (SSVF) and the Emergency Solutions Grant. The user license and standard reporting license will be offered at no cost to all agencies with mandatory participation. Agencies are limited to one reporting license at no cost for every five HMIS ServicePoint users in their agency. Additional licenses can still be purchased using the fee schedule below.

License Type	Description	Annual Fee
Advanced Reporting Tool Licenses (ART)	Optional	$91 per user
Advanced Reporting Tool (ART) Ad Hoc License	Optional and rare	$171 per user

Minimum Data Standards

Minimum Data Collection Standard

All program participation in HMIS, both mandatory and voluntary, is required to collect the following data elements.

- For All Clients: Name
  Social Security Number (Last 4 digits)
  Date of Birth
  Race
  Ethnicity
  Gender
  Disabling Condition
  Destination

- For All Adults: Veteran Status
  Client Location
  Living Situation

Other data elements may be required by funders and HMIS can be set up to accommodate those requirements. The elements listed above are only data elements required by Lake County.

Data Completeness Standard

Five (5) percent or less of the value of any required field can remain null in order to satisfy a minimum standard for data collection.

Compliance with the completeness standard will be monitored periodically by the ServicePoint® System Administrators. Any required fields that have a null value of over 5% must be corrected by the agency with 15 business days of their receipt of the report.

Data Timeliness Standard

In order for data in HMIS to be useful, it must be entered in the system as close to the actual service as possible. All agencies will certify that all clients served within 7 days have been entered into the software system (as applicable). Agencies will also certify that all clients who leave a program will be exited from the software system within 7 days. Night-by-Night shelter providers and street outreach providers must exit clients who have not been in contact with the respective program for 30 days and 90 days respectively.

Data Correctness Standard

HMIS needs to accurately reflect information about clients served at any point in time. Agencies need to monitor data for correctness throughout the year.

Addressing Non-Compliance with Data Standards

Agency Administrators are expected to monitor compliance to the data completeness, timeliness and correctness standards. In addition, System Administrators will run data quality reports to monitor compliance. If an issue is identified, it will be brought to the attention of the agency administrators to be corrected within 15 business days. Agencies will be provided additional training at their request. Agencies may be provided additional training, be asked to submit additional reports or work directly with System Administrators to correct the issue. In cases of repeated noncompliance, System Administrators will report the issue to the Board of Directors for possible action, which may include suspension of your account.

Section 3: Privacy Plan

Client Consent Protocol

Written Client Consent Procedure

As part of the implementation strategy of the system software, a Participating Agency must have client consent procedures and completed forms in place when electronic data sharing is to take place.

Confidentiality and Informed Consent

Informed Consent:

All clients will be provided an oral explanation that their information will be entered into a computerized record keeping system. Participating agencies will provide an oral explanation of the Lake County HMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The agency is also responsible in providing written translation for all legal documents and/or an oral interpreter in the case of a non-English speaking client. The document must contain the following information:

1. What HMIS is

- A web-based information system that homeless services agencies across the county use to capture information about the persons they serve

2. Why the agency uses it

- To understand their clients' needs
- Help the programs plan to have appropriate resources for the people they serve
- To inform public policy in an attempt to end homelessness

3. Security

- Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records

4. Privacy Protection

- No information will be released to another agency without written consent
- Client has the right to not answer any question, unless entry into a program requires it
- Client has the right to know who has added to, deleted, or edited their HMIS record
- Information that is transferred over the web is through a secure encrypted connection

5. Benefits for clients

- Case manager tells client what services are offered on site or by referral through the assessment process
- Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing

Written Client Consent

Each Client whose record is being entered in HMIS and shared electronically with another Participating Agency must agree via a written client consent form to have their data shared. A client must be informed what information is being shared and with whom it is being shared.

Notice of Privacy Practices

All participating agencies **must** post a Notice of Privacy Practices. Agencies may use the sample notice in the appendix or a notice of their own making. Notices must comply with all applicable State and Federal laws.

Information Security Protocols

Information Release

Participating agencies agree not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent. Client consent can be obtained through the standard client consent form included in the appendix or through an additional consent form that identifies the information to be shared and the agencies with which that information will be shared.

Federal/State Confidentiality Regulations

Participating agencies will uphold Federal and State confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

The McKinney-Vento Homeless Assistance Act also regulates disclosure of Protected Personal Information and Participating Agencies must conform to those regulations as contained in the Lake County ServicePoint® Data Services Agreement.

Information Security Protocols

Participating agencies must comply with the following minimum information security protocols:

1. Unique user accounts will be assigned to every user on HMIS. User passwords will not be shared.
2. Users must take all reasonable means to keep password information physically secure. Workstations will not be left unattended with HMIS open. Users must log-off of HMIS before leaving the work area.
3. Users will only share information with individuals who can view information in the HMIS system, are authorized users and the clients to whom the information pertains. Users will only view, obtain, disclose, or use the database information that is necessary to perform job duties. Client information will only be shared in a manner consistent with the signed consents and releases of information by the client.
4. Failure to log off HMIS appropriately may result in a breach in client confidentiality and system security.
5. Hard copies of HMIS information must be kept in a secure file. When hard copies of HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality.
6. If users notice or suspect a security breach, they must immediately notify the Agency Administrator for HMIS or the Lake County System Administrator.

In addition to the Privacy Plan, the following Security Plan will further protect client information from unauthorized information sharing.

Section 4: Security Plan

Security Protocols

Access Levels for System End Users

End User accounts will be created and deleted by the Agency Administrator under authorization of the Participating Agency's Accountability Officer.

Designation of ServicePoint® End Users

Each End User's access level should be reflective of the access he/she has to client level paper records and should be need-based. Need exists only for those shelter staff, volunteers, or designed personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities. It is the responsibility of the Agency's Accountability Officer to approve any and all Agency Administrators in HMIS for their organization.

Access to Data

1. *End User Access:* The HMIS software system contains built-in security measures that restrict agencies from viewing each other's data. End Users will only be able to view the data entered by their own agency or with agencies that agree to share data with the consent of the client.

2. *Raw Data:* End Users who have been granted access to the HMIS Report Writer and Advanced Reporting Tool (ART) have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the HMIS server to an agency's computer, the data become the responsibility of the agency. A Participating Agency should develop protocol regarding the handling of data downloaded from the Report Writer and Advanced Reporting Tool (ART).

3. *Agency Policies Restricting Access to Data:* Participating Agencies must establish internal access to data protocols. Issues to address include storage, transmission, and disposal of data. The policy must include:

    a. Who has access to data

    b. For what purpose they may access data

    c. How data can be transmitted shared

Any and all devices (thumb drives, smart phones, tablets, laptops, computers, etc.) accessing ServicePoint® to download identifying client information must be employee-owned as well as password protected. Any and all electronic documentation or folders (MS Word, PDF, MS Excel Spreadsheet, Shared Employee Folders, the Cloud, etc.), downloaded and/or stored from ServicePoint® with identifying client information (SSN and/or Client First or Last Name), must be password protected and encrypted.

4. *Access to ServicePoint Data:* Access will be granted based upon the following policies developed by the HMIS Committee:

Client-Level Data

This data is only available to the Partner Agency inputting the data, and any other Partner Agency with which there is written consent of the client whose information is to be shared.

If access to client-level data is desired, the interested party should make a formal request, in writing, to the HMIS Committee. This request should include:

- Who is requesting the information
- For what purpose the information is sought
- Specific date range of information requested
- All parties with whom this information will be shared

The HMIS Committee will review all requests for client-level data and make a recommendation to the Board of the Lake County Coalition for the Homeless. The Board will then make a final ruling about whether the information should be shared.

Individual Agency Data

This data may not be shared without the express consent of the Agency's Accountability Officer in question.

Aggregate Data

This data can be used/shared freely by ServicePoint® Partner Agencies, which also includes:

- Lake County Coalition for the Homeless
- ServicePoint® User Group
- Housing and Community Development Commission

HMIS staff should make the HMIS Committee and Board aware of requests for aggregate data from a Non-Partner Agencies.

5. Access to Client Paper Records

Participating Agencies will establish procedures to handle access to client paper records.

Procedures must include:

- Identify which staff has access to the client paper records and for what purpose.
- Staff may only have access to records of clients that they directly work with or for data entry purposes.
- Identify how and where client paper records are stored.
- Develop policy regarding length of storage and disposal procedure of paper records.
- Develop policy on disclosure of information contained in client paper records.

Right to Deny End User and Participating Agencies' Access

Participating Agency or End User access to ServicePoint® may be suspended or revoked for suspected or actual violation of security protocols.

1. All potential violations of any security protocols will be investigated.
2. Any Participating Agency found to have violated security protocols may have their system access suspended or revoked.
3. Any End User found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to:
   - A formal letter of reprimand
   - Suspension of system privileges
   - Revocation of system privileges
   - Criminal prosecution

All sanctions are imposed by and appealed to the Lake County HMIS Committee.

Data Access Control

Agency Administrators at Participating Agencies and Lake County staff must regularly review End User access privileges. Identification codes and passwords must be removed from their systems when End Users no longer require access.

Agency Administrators at Participating Agencies and Central Server staff must implement discretionary access controls to limit access to Lake County HMIS information when available and technically feasible.

Participating Agencies and Lake County HMIS staff must audit all unauthorized accesses, and attempts to access, Lake County HMIS information. Participating Agencies and Lake County HMIS staff also must audit all off-campus accesses, and attempts to access, the Lake County HMIS system. Audit records shall be kept at least six months, and Lake County HMIS staff shall regularly review the audit records for evidence of violations or system misuse.

Guidelines:

- Access to computer terminals within restricted areas should be controlled through a password and/or physical security measures.
- Each End User should have a unique identification code.
- Each End User's identity should be authenticated through an acceptable verification process.
- Passwords are the individual End User's responsibility.
- End Users **cannot** share passwords.
- End Users must be able to select and change their own passwords.
- Passwords must be changed at least every forty-five (45) days.
- Password cannot be re-used until at least 2 password selections have expired.

Auditing: Monitoring, Violations and Exceptions

1. Monitoring
   - Monitoring compliance is the responsibility of Lake County HMIS staff in consultation with the HMIS Committee.
   - All End Users and custodians are obligated to report suspected instances of noncompliance to their Agency Administrators or Lake County HMIS staff as appropriate.
2. Violations
   - Lake County HMIS Staff and the HMIS Committee will review standards violations and recommend corrective and disciplinary actions.
   - End Users should report security violations to an Agency Administrator, or a Lake County HMIS staff person as appropriate.
3. Exceptions
   - Any authorized exception to this policy must be issued from the HMIS Committee and the Participating Agency's Executive Director.

4. Data Logs
   - ServicePoint® maintains an audit trail that will track client-related activity. Any time a client page is added, edited, deleted, or viewed by a ServicePoint® End User, that information will be logged within the system.

Data Assessment and Access

1. Data Classifications

   All data must be identified according to one of the following classifications:

   - Public Data - Information published according to attached Access to Data Subcommittee Recommendations to the Lake County HMIS Committee.
   - Internal Data - Information scheduled, but not yet approved, for publication. Examples include:
     - Draft reports
     - Fragments of data sets
     - Data without context
   - Restricted Data - Information that will never be scheduled for publication. Examples include:
     - Data sets unassociated with any official project
     - Data sets that have not been analyzed
   - Confidential Data - Information that can be used to identify clients contained within the database. Examples include:
     - Name
     - Social security number
     - Address
     - Any other information that can be leveraged to identify a client

2. Procedures for transmission and storage of data: All data must be handled according to their classification. Failure to handle data properly is a violation of this policy.

Public Data: Security controls are not required

Internal Data:

- Accessible only to internal employees
- No auditing is required
- No special requirements around destruction of this data are required
- Data must be stored out of plain view
- May be transmitted via internal or first-class mail

Restricted Data:

- Need-to-know access only
- Requires auditing of access
- Must be stored in a secure location
- No special requirements around destruction of this data are required
- If mailed internally, data must be labeled confidential.
- Can be mailed first-class.

Confidential Data:

- Requires encryption at all times
- Hard copies of this data should never be produced
- Data must be magnetically overwritten, and destruction must be verified by Database Administrator
- Cannot be mailed and may only be delivered *by hand* to data owner

Data Integrity Controls

Controls must exist to ensure data remain consistent with their source.

Data integrity controls must encompass both manual and electronic processing. All discovered errors, duplications, omissions, and intentional alterations should be investigated. Many data integrity controls will reside within the application or system.

All client identifiable information will be encrypted and stored on the Central Server.

Local Data Storage

Client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the Participating Agency.

Each Participating Agency should develop policies consistent with Information Security Policies outlined in this document regarding client-identifying information stored on local computers.

Electronic Transmission of Authenticators

Central Server staff and Participating Agencies will not engage in electronic transmission of End User ID's and passwords, except for first-time or temporary passwords. Authenticators will be transmitted only by telephone, mail, or in person.

Appendices

Appendix A

DATA SERVICES AGREEMENT

(See Below)

SERVICEPOINT® DATA SERVICES AGREEMENT

This Data Services Agreement ("Agreement") is entered into this 1st day of March, 2018 (the "Effective Date") by and between _____ (the "Participating Agency") and Lake County ("LC"), individually (a "Party") and jointly (the "Parties").

WHEREAS, the ServicePoint® Referral Network ("ServicePoint") is an information system that helps improve service delivery and evaluate the effectiveness of services provided;

WHEREAS, LC uses ServicePoint® as its Homeless Management Information System (HMIS). All programs funded under US Department of Housing and Urban Development McKinney-Vento Act as amended by the HEARTH Act or the Emergency Solutions Grant are required to participate in HMIS as a condition of their funding. While HUD does not require providers that do not receive HUD funds to participate in ServicePoint®, LC works closely with non-funded agencies to articulate the benefits of ServicePoint® and strongly encourages their participation in order to achieve a comprehensive and accurate understanding of homelessness and other social service needs in Lake County; and

WHEREAS, Participating Agency and other participating agencies and programs ("Participating Agencies") will be required to comply with all applicable operating procedures and must agree to execute and comply with provisions in this Agreement, regardless of their status as mandatory or voluntary.

THEREFORE, in consideration of the foregoing, the Parties agree to the terms and conditions of the Agreement as set forth below:

1. Definitions. Except as otherwise expressly provided, terms used in this Agreement shall be defined as follows. If not otherwise defined, terms shall have the meaning as defined under HIPAA.
Authorization: The federal and state laws that apply to the requirements of a legal document that allows an individual's health information to be used or disclosed to a third party, the minimum standards are (a) those set forth in the HIPAA Privacy Rule, (b) as modified or superseded by the minimum requirements of applicable federal and state laws applicable to the type of health information to be used or disclosed including, but not limited to, state laws that apply to mental health or Human Immunodeficiency Virus. A template Authorization for use by Participating Agencies is attached hereto as **Exhibit A**.

Confidential Information: Any information, other than Protected Health Information, regarding the business, personnel and operations of a Party or its affiliates, if applicable, and their respective trustees, officers, employees, and volunteers accessed, collected, or obtained as part of this arrangement that is not otherwise publicly known, and may include, but is not limited to, data and information concerning financial operations, service area markets, customer population characteristics, types and numbers of services offered, quality assurance, utilization review, risk management, research, procurement, contracting, trade secrets, intellectual property, proprietary information and other operational information that may provide either (i) the other Party, or (ii) other Participating Agencies, its officers, directors, or employees, a competitive advantage in its relevant markets.

Data Privacy Standards: The federal and state laws and standards, including, but not limited to HIPAA and state laws that apply to mental health or HIV/AIDS.

Data Security Standards: The federal and state laws and standards, including, but not limited to HIPAA and NIST standards.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and all implementing regulations, including the HIPAA Privacy Rule and HIPAA Security Rule, as may be amended from time to time.

Participating Agencies: Institutions and organizations that have received official approval by the ServicePoint® Coordinating Council (or its designee) to exchange information within ServicePoint® by entering into this or a substantially similar Data Services Agreement with LC.

Participating Agency Information: Information obtained from, created by or for, or disclosed by a Participating Agency that includes Protected Health Information and is exchanged utilizing ServicePoint®

ServicePoint Coordinating Council: The governing body that acts of behalf of Participating Agencies for purposes of operating ServicePoint®.

2. ServicePoint Terms

LC shall enter into Data Services Agreements, substantially similar in terms and conditions as this Agreement with Participating Agencies. The Parties agree that any proposed changes to the terms of the ServicePoint® Data Services Agreement entered into with proposed Participating Agencies must be approved by the ServicePoint® Coordinating Council. Participating Agency understands that each of the other Participating Agencies are third party beneficiaries to this Agreement. LC represents that Participating Agency is a third-party beneficiary to each ServicePoint® Data Services Agreement.

3. ServicePoint® Minimum Data Structure, Communication, & Administrative Requirements

Participating Agency shall comply with and implement the data model utilized by ServicePoint®. LC will notify Participating Agency of any updates or changes to the data model. If Participating Agency Information is in a format that is not consistent with the data model, LC will notify Participating Agency and the Parties will discuss and work collaboratively and in good faith to resolve any discrepancies.

4. Uses, Disclosures, Maintenance, Access, and Storage by Participating Agency.

Participating Agency warrants and shall ensure its uses, disclosures, maintenance, access, and storage of Participating Agency Information and other data derived from Participating Agency Information to or from LC and through ServicePoint® are based on the appropriate permissions and approvals or are otherwise allowed by law. Participating Agency shall be responsible for its own uses, disclosures, maintenance, access, and storage of Participating Agency Information and its other data derived from Participating Agency Information. Participating Agency acknowledges and agrees that LC is relying upon Participating Agency's representation herein that it will ensure compliance with all federal and state laws applicable to the use, disclosure, maintenance, access, and storage of Participating Agency Information. Participating Agency shall defend, indemnify, and hold LC harmless from any damages, claims, demands, or actions arising out of or related to Participating Agency's failure to comply with applicable law. In addition to this Agreement, Participating Agency and LC shall enter into the Business Associate Agreement in the form set forth as **Exhibit B**.

5. Security Notification.

Participating Agency shall notify LC of any event of an attempted or successful unauthorized access, use, disclosure, modification, destruction, or alteration of the data within Participating Agency's facility or network, purported HIPAA violation or breach, or other incident of technical intrusion or suspected malicious operational disruption that could potentially impact ServicePoint®, LC, or other Participating Agencies as soon as possible (and no later than 10 days) after discovery. Participating Agency agrees to cooperate with LC's and other Participating Agencies' reasonable requests in response to each incident, violation, or breach.

6. Participating Agency Information Use Requirements

Participating Agency and LC each represent it has, and will continue to, adopt, follow, and/or enforce (as applicable) Data Privacy and Data Security Standards in accordance with applicable law. Participating Agency will ensure its workforce is trained on the appropriate use and disclosure of protected health information on at least an annual basis. Participating Agency will ensure that any Notice of Privacy Practices utilized for individuals receiving services within ServicePoint includes and complies with the terms and conditions set forth in this Agreement. Participating Agency shall provide reasonable access to LC in the event that LC is required by applicable law to carry out security audits and reviews of ServicePoint®.

LC agrees to use appropriate safeguards to prevent use or disclosure of Participating Agency Information or information derived from Participating Agency Information other than as permitted under this Agreement.

7. LC Security Notification.

LC shall notify Participating Agency of any attempted or successful unauthorized access, use, disclosure, modification, destruction, or alteration of unsecured Participating Agency Information, purported HIPAA violation or breach, or other incident of technical intrusion or suspected malicious operational disruption. LC shall notify Participating Agency of the incident as soon as possible (and no later than 10 days) after discovery. LC agrees to cooperate with Participating Agency's reasonable requests in response to each incident.

8. Use of Participating Agency Information.

LC is only permitted to request, receive, store, and use Participating Agency Information and other data derived from Participating Agency Information pursuant to this Agreement and LC shall not use such information for any other purposes unless allowed by law. To further the purposes of ServicePoint, LC may store Participating Agency Information in a secure data warehouse integrated with ServicePoint in accordance with Data Privacy Standards, Data Security Standards, and applicable law.

9. User Policy, Responsibility Statement & Code of Ethics.

Participating Agency will comply with the terms and conditions and ensure that each member of its workforce complies with the terms and conditions of the User Policy, Responsibility Statement & Code of Ethics, attached hereto as **Exhibit C**.

10. Disclosures Required by Law.

If disclosure of Participating Agency Information is required by law, court order, subpoena, administrative process, or other similar requirement, then LC shall provide maximum practical advanced notice to

Participating Agency to allow it to obtain a protective order or otherwise limit the dissemination of Participating Agency Information, at Participating Agency's sole expense. In circumstances involving a disclosure by LC of Participating Agency Information for public health reporting purposes, LC is not obligated to provide such advance notice to Participating Agency and Participating Agency agrees that such disclosures may take place without notice or opportunity to object, in accordance with state and federal law.

11. Term and Termination.

The term of this Agreement shall commence as of the Effective Date and continue for four (4) years (the "Term"), unless earlier terminated as follows:

A. Mutual agreement of the Parties in writing to terminate this Agreement,
B. Upon sixty (60) days' advance written notice of termination by either Party, with or without cause,
C. Upon thirty (30) days' advance written notice of breach of this Agreement by either Party describing the alleged breach with sufficient information to identify it, if the other Party fails to cure the breach.

Upon termination and the request of Participating Agency, LC will (i) return or destroy all Participating Agency Information except where such return or destruction is not feasible or to the extent necessary to comply with retention periods of this Agreement, including as they pertain to Participating Agency Information and (ii) cooperate with Participating Agency to transition any information that Participating Agency determines it must retain in support of its operations and research. In the event return or destruction of the Participating Agency Information is not feasible, then LC will extend the protections of this Agreement to the Participating Agency Information and limit further uses and disclosures to those purposes that make the return or destruction of the Participating Agency Information infeasible.

12. Fee Schedule.

Participating Agency shall pay to LC the user fees as set forth in **Exhibit D**.

13. Confidentiality.

No Confidential Information of a Party, in whatever form, accessed, collected, maintained, or used shall be disclosed by the other Party except as and only to the extent specifically permitted by this Agreement and to the extent permitted by law. If dissemination of Confidential Information is required by law, the Party required disclosing Confidential Information shall provide maximum practical advance notice to the other Party to allow it to obtain a protective order or otherwise limit the dissemination of their Confidential Information, at their sole expense.

The Parties agree that they will not use in any way the names, trademarks, logos, symbols, or a description of the business or activities of each other without in each instance obtaining prior written consent. These uses include, but are not limited to, promotional, informational, and marketing activities and materials. The existence of this Agreement shall not constitute an implied endorsement of any products or services offered by either Party.

14. LIMITATION OF LIABILITY.

ALL PARTICIPATING AGENCY INFORMATION OR ANY FORM OR DERIVATIVE THEREOF IS BEING PROVIDED BY PARTICIPATING AGENCY AND BY LC "AS IS," AND PARTICIPATING AGENCY, LC, AND EACH OF THEIR LICENSORS, EMPLOYEES AND AGENTS OR AFFILIATES EXPRESSLY DISCLAIM TO THE MAXIMUM EXTENT

PERMITTED BY LAW, ALL WARRANTIES, OTHER THAN WARRANTIES CONTAINED IN THIS AGREEMENT, WHETHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, (i) ANY WARRANTY THAT ANY CONTENT, DELIVERABLES OR SERVICES ARE ACCURATE OR RELIABLE, (ii) ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND (iii) ANY AND ALL IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. NO ADVICE, STATEMENT OR INFORMATION GIVEN BY PARTICIPATING AGENCY, LC, THEIR AFFILIATES, CONTRACTORS OR EMPLOYEES SHALL CREATE OR CHANGE ANY WARRANTY PROVIDED HEREIN.

NEITHER PARTICIPATING AGENCY OR ITS AFFILIATES, NOR LC, NOR THEIR RESPECTIVE AGENTS OR EMPLOYEES WILL BE LIABLE TO EACH OTHER FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY PUNITIVE, TREBLE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS, REVENUE, PROFITS, STAFF TIME, GOODWILL, USE, DATA, OR OTHER ECONOMIC ADVANTAGE), WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, WHETHER OR NOT PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15. Miscellaneous Terms.

A. The Parties will undertake reasonable procedures to ensure that employees and contractors have not been debarred, suspended, excluded, or otherwise become ineligible to participate in any government health care program, and that it is not excluded from any government health care program.

B. Neither Party may assign, subcontract, delegate or otherwise transfer any of its rights or obligations hereunder, nor may it contract with third parties to perform any of its duties or obligations hereunder, without the other Party's prior written consent. Any attempt to take such action(s) without consent shall be void.

C. The Parties are independent contractors of each other. Nothing contained in this Agreement shall constitute, or be construed to create, a partnership, joint venture, agency or any other relationship other than that of independent contractors to this Agreement.

D. Any notice required or permitted to be given under this Agreement shall be sufficient if in writing and delivered or sent via nationally recognized overnight mail service, signature required, or Registered or Certified United States Mail, return receipt requested, postage prepaid:

If to Participating Agency: If to LC:

E. This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the State of Illinois.

F. If any portion of this Agreement shall for any reason be invalid or unenforceable, such portion shall be ineffective only to the extent of such invalidity or unenforceability, and the remaining portions shall remain valid and enforceable and in full force and effect.

G. This Agreement may be executed in any number of counterparts, each of which will be considered an original as against the Party whose signature appears thereon, but all of which taken together will constitute one and the same instrument.

H. This Agreement, including all attachments and exhibits hereto, sets forth the entire agreement between the Parties relative to the subject matter of this Agreement. Any representations, promises, or conditions, whether oral or written, not incorporated in this Agreement shall not be binding upon either Party.

IN WITNESS WHEREOF, the Parties have caused this ServicePoint® Data Services Agreement to be executed by their respective duly authorized representatives as of the Effective Date.

PARTICIPATING AGENCY:	**LC:**
_____	**Lake County**
By: _____	By: _____
Its: _____	Its: _____

Appendix B

Exhibit A

AUTHORIZATION

(See Below)

Authorization to Share Information Using ServicePoint®

In order to provide faster and more definitive linkages to needed services, Lake County utilizes a computer system called "ServicePoint®." ServicePoint® is an information system that helps us improve service delivery and evaluate the effectiveness of services provided. The ServicePoint® system will be shared among Lake County agencies that have signed an agreement with Lake County and are participating in ServicePoint® (the "Participating Agencies").

TO WHOM INFORMATION WILL BE DISCLOSED TO AND RECEIVED FROM VIA SERVICEPOINT®:

- Employees and staff of this Participating Agency
- Participating Agencies in ServicePoint®. A listing of the Participating Agencies is available to you upon request. A more frequently-updated listing can be found at www.lakecountyil.gov/1957/ServicePoint, which is subject to change. You may also obtain the most current listing by requesting a copy from this Participating Agency
- The ServicePoint® System Administrators at Lake County have access to information for the purpose of maintaining the database

SPECIFIC INFORMATION THAT WILL SHARED VIA SERVICEPOINT®:

By signing this document, you understand that the following information (the "Protected Health Information") may be used and disclosed by and among the Participating Agencies:

- Name
- Social Security number
- Demographics
- Contact information
- Emergency contact information
- Case manager contact information
- Employment and education information
- Residential and homeless history
- Income, employment and benefit information
- Health insurance and provider
- Information on service referrals
- ServicePoint agency engagement including intake and exit dates
- Basic identifying information on other household members

Your information may be shared by and among Participating Agencies to facilitate the services we provide you and to better serve you and your needs.

- You can revoke this authorization at any time by writing to the Participating Agency which provided you a service.
- You understand that your revocation is not effective to the extent Lake County and/or a Participating Agency has relied on this authorization to store, use or disclose your Protected Health Information.
- If you revoke this consent, no further Protected Health Information will be entered in or used and/or disclosed with Participating Agencies through ServicePoint®.
- We will not condition any services, treatment or any payment(s) on whether you sign this authorization.
- You agree to discuss any questions and/or concerns with the Participating Agency and that you will be provided a signed copy of this authorization.
- You understand that information disclosed pursuant to this authorization may be redisclosed and may no longer be protected by applicable state or federal law.

I have read and understand the above material and I hereby consent that Lake County and the Participating Agencies use, disclose, enter, transmit, and share the Protected Health Information for me or my child(ren)/ward(s)/dependent(s) identified below using ServicePoint® and, if I am between the ages of 13-17, to share Protected Health Information with my parent or guardian.

Client/Parent/Guardian (Signature) Date	Employee Signature Date
Print Name	Print Name
Address	Title/Agency

City State Zip Code

Child/Dependent/Ward

This Authorization expires on_____, 20__.

Child/Dependent age 13-17 (Signature)

Autorización para Compartir Información Usando ServicePoint®

Para proporcionar vínculos más rápidos y más definitivos a los servicios necesarios, Lake County utiliza un sistema de computadora llamado "ServicePoint ®." El sistema ServicePoint ® es un sistema de información compartido entre agencias en el condado de Lake que han firmado un acuerdo con Lake County y participan en ServicePoint® (la "Agencia Participante").

A QUIEN SE DIVULGARA Y QUIEN RECIBIRA LA INFORMACION DE SERVICEPOINT®:

- Empleados y personal de esta Agencia Participante
- Agencias que Participan en ServicePoint®. Una lista de Agencias Participantes estará disponible para usted a petición. Puede encontrar una lista actualizada con más frecuencia en www.lakecountyil.gov/1957/ServicePoint, que está sujeta a cambios. También puede obtener una lista más actual solicitando una copia de esta Agencia Participante.
- El Administrador de ServicePoint® de Lake County tiene acceso a la información con el fin de mantener la base de datos

INFORMACION ESPECIFICA QUE SE COMPARTIRA A TRAVES DE SERVICEPOINT®:

Al firmar este documento, usted entiende que la siguiente información (la "Información de Salud Protegida") puede ser usada o divulgada por y entre las Agencias Participantes:

- Nombre
- Número de seguro social
- Información demográfica
- Información de contacto
- Información de contacto en caso de emergencia
- Información de contacto de coordinador de servicios
- Información de empleo y educación
- Historia residencial y sin hogar
- Información de ingreso, empleo, y beneficios
- Seguro médico y proveedor de servicios médicos
- Información sobre referencias de servicios
- Información sobre participación en agencias de ServicePoint incluyendo fechas de entrada y salida
- Información básica sobre la identificación de otros miembros del hogar

Su información puede ser compartida por y entre Agencias Participantes para facilitar los servicios que le proveemos y para mejor servir sus necesidades.

- Usted puede revocar esta autorización en cualquier momento escribiéndole a la Agencia Participante que le proveo el servicio.
- Usted entiende que su revocación no es efectiva en la medida en que Lake County y/o la Agencia Participante hayan confiado en esta autorización para almacenar, usar o divulgar su Información de Salud Protegida.
- Si revoca este consentimiento, no se ingresará ni utilizará y/o divulgará más información de salud protegida con las agencias participantes a través de ServicePoint®.
- No condicionaremos ningún servicio, tratamiento, o pago alguno sobre si usted firma esta autorización.
- Usted acepta discutir cualquier pregunta y/o inquietud con la Agencia Participante y que se le proporcionara una copia firmada de esta autorización.
- Usted comprende que la información divulgada conforme a esta autorización puede volver a divulgarse y puede que ya no esté protegida por la ley estatal o federal aplicable.

He leído y entiendo el material anterior y doy mi consentimiento para que Lake County y las Agencias Participantes usen, divulguen, ingresen, transmitan y compartan la información de salud protegida para mi o mi hijo(s)/ pupilo(s)/ dependiente(s) identificado(s) a continuación utilizando ServicePoint® y, si tengo entre 13 y 17 años, para compartir Información de Salud Protegida con mis padres o tutores.

Cliente/Padre/Guardian (Firma)	Fecha	Firma de Empleado	Fecha
Nombre en Letra Imprenta		Nombre en Letra Imprenta	
Dirección		Titulo/Agencia	

Cuidad Estado Código Postal

Hijo(s)/ Pupilo(s)/ Dependiente(s)

Esta Autorización expira _____, 20__.

Hijo/Dependiente Edad 13-17 (Firma)

Appendix C

EXHIBIT B

BUSINESS ASSOCIATE AGREEMENT

(See Below)

BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into this ____ day of _____, 201__ (the "Effective Date"), by and between _____ ("Covered Entity") and Lake County ("Business Associate"), (collectively, the "Parties").

WHEREAS, Covered Entity is a "Covered Entity" as that term is defined in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended ("HIPAA"), and the Privacy, Security, Breach, Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164 (jointly "HIPAA Rules") promulgated thereunder;

WHEREAS, Business Associate is a "Business Associate" as that term is defined in the HIPAA Rules, and may access, use, create, maintain, transmit, receive and/or disclose Protected Health Information ("PHI") of the Covered Entity;

WHEREAS, pursuant to the HIPAA Rules, the Business Associate must agree in writing to certain mandatory provisions and must comply with HIPAA and the HIPAA Rules.

NOW, THEREFORE, in consideration of the mutual covenants and promises set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

ARTICLE I
DEFINITIONS

1.1 Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules.

1.2 All PHI that is created or received by the Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording and electronic display, by Covered Entity or its operating units to Business Associate, or is created, maintained, accessed, transmitted, used, disclosed, or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

ARTICLE II
PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

2.1. Business Associate may use, access, create, maintain, transmit, receive and disclose PHI as reasonably required or contemplated in connection with the performance of services provided to or on behalf of Covered Entity as specified in a separate agreement between the parties, excluding the use or further disclosure of such PHI in a manner that would violate the requirements of the HIPAA Privacy Rule, if done by the Covered Entity.

2.2 Business Associate may use and disclose such PHI for the proper management and administration or to carry out the legal responsibilities of Business Associate.

2.3. Business Associate agrees it will not use or further disclose PHI other than as permitted or required by this Agreement or as required by applicable law.

2.4. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for in this Agreement.

2.5. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware.

2.6. Business Associate agrees to ensure that any subcontractors that create, receive, maintain, use, disclose, access or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information. Business Associate agrees to satisfy this requirement by implementing a written agreement with each subcontractor setting forth the terms and conditions required under this Agreement.

2.7. In the event Business Associate maintains a Designated Record Set, within ten (10) days of a Covered Entity's request for access to PHI in a Designated Record Set held by Business Associate, Business Associate agrees to provide reasonable access (including inspection and obtaining copies to such Covered Entity in order to meet the requirements of the HIPAA Privacy Rule.

2.8. In the event Business Associate maintains a Designated Record Set, it will, at the request of the Covered Entity, make available to Covered Entity within ten (10) days the PHI in a Designated Record Set held by Business Associate for amendment and immediately incorporate any amendments to such information in accordance with the HIPAA Privacy Rule.

2.9. To the extent feasible, Business Associate will maintain and, within ten (10) days following the request of Covered Entity, make available to Covered Entity the information possible to assist Covered Entity in providing an accounting of disclosures in accordance with the HIPAA Privacy Rule. Business Associate does not currently possess the technology at this time to provide Covered Entity with an accounting of disclosures.

2.10. In the event that Business Associate receives a request from an Individual or patient for Access, Amendment or Accounting purposes as described in Sections 2.7 – 2.9 above, Business Associate will immediately notify Covered Entity in writing of said request and provide reasonable assistance to Covered Entity in responding to said request in a timely fashion so as to permit Covered Entity to respond to the request within the time limits imposed under the HIPAA Rules and in any event, no later than ten (10) days following the request. Covered Entity will have sole and exclusive authority in overseeing the response to an Individual's or patient's request and Business Associate will not provide any response to an Individual or patient without first notifying Covered Entity in writing and complying with the reasonable instructions from Covered Entity.

2.11. Business Associate will make its internal practices, books, and records relating to the use and disclosure of such PHI available to the Secretary of the U.S. Department of Health & Human Services ("HHS") for purposes of determining the Covered Entity's and Business Associate's compliance with HIPAA and the HIPAA Rules. In the event that Business Associate receives a request from HHS or any other state or federal agency relating to PHI, Business Associate will provide immediate notice to Covered Entity and grants Covered Entity authority to direct the response to any such request to the extent it relates to PHI of Covered Entity.

2.12. Business Associate will, at termination of this Agreement, return or destroy all PHI that Business Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, extend the protections of this Agreement to PHI and limit further uses and disclosures to those purposes that make the return or destruction of such PHI infeasible.

ARTICLE III
RESPONSIBILITIES OF BUSINESS ASSOCIATE

3.1. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity as required under the HIPAA Security Rule.

3.2. Business Associate will immediately report to Covered Entity any successful unauthorized access, use, disclosure, modification, or destruction of electronic PHI or interference with system operations in an Information System affecting such electronic PHI of which Business Associate becomes aware.

3.3. Business Associate will ensure that any agent, including a subcontractor, to whom it provides such electronic PHI enters into a written agreement with Business Associate and agrees to implement reasonable and appropriate safeguards to the same extent required by Business Associate under this Agreement.

3.4. Breach Notification.

3.4.1. Business Associate will report to Covered Entity in writing any acquisition, access, use or disclosure of PHI in violation of HIPAA which could be or is considered a Breach of Unsecured PHI within ten (10) days of discovery of the Breach.

3.4.2. Business Associate will fully cooperate with Covered Entity to investigate, mitigate, assess any risk, resolve, and notify any Individuals, media, and HHS as determined necessary by Covered Entity. Covered Entity will have sole discretion in addressing and responding to any purported Breach.

3.5. To the extent Business Associate agrees to carry out one or more of Covered Entity's obligation(s) under the HIPAA Rules, Business Associate will comply with such requirements of the HIPAA Rules that apply to Covered Entity in the performance of such obligation(s).

3.6. Business Associate relies upon Covered Entity to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures and Business Associate will rely upon Covered Entity to use or disclose the minimum necessary PHI when carrying out its obligations to provide the Services.

3.7. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.8. Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Business Associate or Covered Entity related to the use, access, disclosure, transmission, reception, creation, or maintenance of PHI by Business Associate.

ARTICLE IV
RESPONSIBILITIES OF COVERED ENTITY

4.1. Covered Entity will notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

4.2. Covered Entity will notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under the HIPAA Privacy Rule, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4.3. Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity, except for use or disclosure of PHI for management and administration or to carry out legal responsibilities of Business Associate. Covered Entity acknowledges that Business Associate is relying upon Covered Entity to use or disclose only the minimum necessary information.

ARTICLE V
TERM AND TERMINATION

5.1. Term. The Term of this Agreement shall become effective on the Effective Date and shall continue for so long as Business Associate creates, uses, discloses, maintains, transmits, or receives PHI on behalf of Covered Entity.

5.2. Termination. If either Party fails to perform any material obligation pursuant to this Agreement, and (i) cure of the failure to perform the material obligation is possible and the failure to cure continues for a period of ten (10) days after the breaching Party is notified in writing by the non-breaching Party of said failure to perform, or; (ii) cure is not possible, then the non-breaching Party may terminate the Agreement immediately by written notice of same to the breaching Party. Covered Entity, if the non-breaching Party, may also terminate any other agreement between the parties that involves the use or disclosure of PHI, in the event that Business Associate has failed to perform any material obligation pursuant to this Agreement. In addition, Covered Entity may terminate this Agreement without cause upon thirty (30) days written notice to Business Associate.

5.3. Obligations of Business Associate Upon Termination.

5.3.1. Upon termination of this Agreement for any reason, upon request of Covered Entity Business Associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all PHI created, maintained, used, disclosed, transmitted or received from Covered Entity that Business Associate still maintains in any form. Business Associate shall retain copies of the PHI to the extent necessary to address legal, regulatory, and risk management processes and requirements.

5.3.2. If the return or destruction of PHI by Business Associate is not feasible, Business Associate will then extend the protections of this Agreement to the PHI and to limit further use.

5.3.3. The obligations set forth hereunder shall apply to all subcontractors of Business Associate that create, maintain, exchange, or receive PHI from Business Associate and Business Associate will take all necessary action to ensure that each such subcontractor complies with these provisions upon termination.

5.3.4. The obligations of Business Associate and each of its applicable subcontractors under this Section shall survive the termination of this Agreement.

ARTICLE VI
MISCELLANEOUS

6.1 Regulatory Reference. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

6.2 Preemption. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Rules, as amended, the HIPAA Rules shall control. In the event of an inconsistency between the provisions of the HIPAA Rules and other applicable confidentiality laws, the provisions of the more restrictive rule will control.

6.3 Independent Entities. None of the provisions of this Agreement is intended to create, nor shall any be construed to create, any relationship between the Parties other than that of independent entities contracting with each other solely to effectuate the provisions of the Agreement.

6.4 Severability. The invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of any other term or provision.

6.5 Amendments. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA Rules or any more restrictive State law and any future regulations, statutes or other guidance concerning HIPAA that may affect this Agreement.

6.6 No Third-Party Beneficiaries. This Agreement shall not in any manner whatsoever confer any rights upon or increase the rights of any third-party.

6.7 Survival of Terms. The obligations of Business Associate under Articles II, III, V, and VI of this Agreement shall survive the expiration, termination, or cancellation of this Agreement and shall continue to bind Business Associate, its agents, employees, subcontractors, successors, and assigns as set forth herein.

6.8 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Rules.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

BUSINESS ASSOCIATE:	COVERED ENTITY:
Lake County	_____
By: _____	By: _____
Its: _____	Its: _____

Appendix D

EXHIBIT E

USER POLICY, RESPONSIBILITY STATEMENT & CODE OF ETHICS

(See Below)

User Policy, Responsibility Statement & Code of Ethics

For Lake County's ServicePoint®

User Policy

Partner Agencies shall share information for the purposes of coordinating services to individuals enrolled in ServicePoint®. Aggregate non-identifying data may also be used for reporting unduplicated counts to state, federal and other funding sources. Lake County seeks to establish a uniform, consistent, and accurate source of data for all member participants and stakeholders.

It is a Client's decision about which information, if any, entered into the ServicePoint® system shall be shared and with which Partner Agencies. The *Consent To Use ServicePoint®* must be signed if the Client agrees to share basic information with Partner Agencies. A separate *Release of Information* form must be signed if the Client agrees to share anything other than basic identifying information.

The ServicePoint® system is a tool to assist agencies in focusing services and locating alternative resources to help clients. Therefore, agency staff should use the Client information in the ServicePoint® system to target services to the Clients' needs.

To the greatest extent possible, data necessary for the development of aggregate reports of homeless services, including services needed, services provided, referrals and client goals and outcomes should be entered into the system in a timely and accurate manner.

Users Code of Ethics

A. The ServicePoint® User has primary responsibility for his/her Client(s).
B. Each ServicePoint® User should maintain high standards of professional conduct in the capacity as a ServicePoint® User.
C. ServicePoint® Users must treat Partner Agencies with respect, fairness and good faith.
D. ServicePoint® Users have the responsibility to relate to the Clients of other Partner Agencies with full professional consideration.

Strong Password Protocols

Minimum length of eight characters which:

- Are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, dates of birth, etc.
- Are free of consecutive identical characters or all-numeric or all-alphabetical groups
- Are free of word or number patterns
- Are not names or words in any dictionary including English, foreign languages, and technical dictionaries (legal, medical, etc.)
- Contains at least one uppercase letter, one lowercase letter, and 2 numbers

User Responsibility

Your User ID and Password give you access to the Lake County ServicePoint® 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 from the ServicePoint® system.

— My User ID and Password are for my use only and must not be shared with anyone.

— I must take all reasonable means to keep my password physically secure.

— I understand that the only individuals who can view information in the ServicePoint® system are authorized users and the Clients to whom the information pertains.

— I may only view, obtain, disclose, or use the database information that is necessary to perform my job.

— I am required to understand and obey all requirements indicated in the *ServicePoint® Business Agreement* and *Notice of Privacy Practices*.

— Each client must be informed of their privacy rights and sign the *Consent to Use ServicePoint®* before sharing information in to the database.

— Client information will only be shared in a manner consistent with the signed consents and releases of information by the client.

— If I am logged Into ServicePoint® and must leave the work area where the computer is located, I **must log-off** of ServicePoint® before leaving the work area.

— A computer that has ServicePoint® open and running shall never be left unattended. Failure to log off ServicePoint® appropriately may result in a breach in client confidentiality and system security.

— Hard copies of ServicePoint® information must be kept in a secure file.

— When hard copies of ServicePoint® information are no longer needed, they must be properly destroyed to maintain confidentiality.

— Hard copies of ServicePoint® information must be kept in a secure file. When hard copies of ServicePoint® information are no longer needed, they must be properly destroyed to maintain confidentiality.

— I will only access ServicePoint® from a computer owned and maintained by my employer.

— If I notice or suspect a security breach, I must immediately notify the Agency Administrator for ServicePoint® or the Lake County System Administrator at 847-377-2331.

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

_____ _____

ServicePoint® User – **Print Name & Sign** Date

_____ _____

Agency Administrator – **Print Name & Sign** Date

Note: Forms should be signed by the User & Agency Administrator, a copy kept on site and a copy delivered to the Lake County ServicePoint® Administrator.

Appendix E

EXHIBIT D

FEE SCHEDULE

(See Page 14)

Appendix F

NOTICE OF PRIVACY PRACTICES

(See below)

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW PRIVACY INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. **PLEASE REVIEW IT CAREFULLY**.

THE PRIVACY OF YOUR PERSONAL INFORMATION IS IMPORTANT TO US.

Purpose of This Notice

ServicePoint® is a centralized case management system that allows authorized participating agency personnel throughout Lake County, Illinois, to collect client data, produce statistical reports, and share information with select partner agencies if a signed "release of information" form is signed by the client.

This notice tells you about how we use and disclose your private personal information. It tells you about your rights and our responsibilities to protect the privacy of your private personal information. It also tells you how to complain to us, or the government if you believe that we have violated any of your rights or any of our responsibilities.

We are required by law to maintain the privacy of your private personal information. We must provide you with a copy of this notice upon request. We must follow the terms of this notice that are currently in effect.

We reserve the right to change this Notice at any time. This Notice is not a legal contract. If this notice is changed, a copy of the revised notice will be available upon request or posted at our location or on our website. We may change our practices and those changes may apply to medical information we already have about you as well as any new information we receive in the future.

Instructions

We must check applicable state privacy law to determine if it provides greater privacy protections or rights than federal law. If so, our Notice must reflect those greater protections or rights. **AGENCY** must approve each Notice of Privacy Practices to ensure that the Notice sufficiently complies with applicable federal and state laws before we may distribute the Notice.

The Notice must be made available upon request to each individual no later than the date of our first service delivery, including service delivered electronically after the compliance date for the federal Privacy Rules established by the Department of Housing and Urban Development. **AGENCY**, or the **AGENCY'S** Business Associates, must also have the Notice available at the service delivery site for individuals to request to take with them. At all physical service delivery sites, the Notice must be posted in a clear and prominent location where it is reasonable to expect any individuals seeking service from the **AGENCY** to be able to read the Notice. Whenever the Notice is revised, make the Notice available upon request on or after the effective date of the revision in a manner consistent with the above instructions. Thereafter, the Notice must be made available upon request to each new client at the time of service delivery and to any person requesting a Notice.

Our Legal Duty

We are required by applicable federal and state law to maintain the privacy of your private personal information. We are also required to make this notice about our privacy practices, our legal duties, and your rights concerning your private personal information available upon request. We must follow the privacy practices that are described in this notice while it is in effect. This notice takes effect immediately, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all private personal information that we maintain, including private personal information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and make the new notice available upon request.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the information listed at the end of this notice.

How We Use or Disclose Your Private Personal Information

To Provide Services

We will use private personal information about you to provide you with services. We may share this information with members of our staff or with others involved in your support. We may also disclose your private personal information to a member of your family or other person who is involved in your care upon your approval.

For Administrative Operations

We may use or disclose your private personal information for operational purposes. For example, we may use your private personal information to evaluate our services, including the performance of our staff in caring for you. We may also use this information to learn how to continually improve the quality and effectiveness of the services that we provide to you.

There are some services that are provided for us by our business associates such as accountants, consultants and attorneys. Whenever we share information with our business associates we will have a written contract with them that requires that they protect the privacy of your private personal information.

Other Uses or Disclosures of Your Personal Information

Service Alternatives – We may use and disclose private personal information about you to contact you about other services that are available to you. If you do not want to receive these communications, please notify our Complaint Officer in writing.

Related Benefits and Services – We may use and disclose private personal information about you to contact you about other benefits or services that may interest you. If you do not want to receive these communications, please notify our Complaint Officer in writing.

Individuals Involved in Your Care – With your approval, we may disclose private personal information about you to a family member, other relative, close friend or any other person identified by you if they are involved in your care. We may also use or disclose private personal information about you to notify those persons of your location, general condition or death. If there is a family member, other relative or close friend to whom you do not want us to disclose private personal information about you, please notify our Complaint Officer in writing.

Uses or Disclosures That Are Required or Permitted by Law

For Administrative Functions - We may use or disclose your protected personal information to carry out the administrative functions of our office.

Academic Research Purposes - We may use or disclose protected personal information to individuals performing academic research who have a formal relationship with ServicePoint®.

Required by Law – We may use or disclose medical information about you when we are required to do so by law.

Public Health Activities – We may disclose private personal information about you if the HMIS user or developer, in good faith, believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

Victims of Abuse, Neglect or Domestic Violence – We may disclose private personal information about you to a government agency if we believe you are the victim of abuse, neglect or domestic violence.

Legal Activities – We may disclose private personal information about you in response to a court proceeding. We may also disclose private personal information about you in response to a subpoena or other legal process.

Disclosures for Law Enforcement Purposes – We may disclose private personal information about you to law enforcement officials for law enforcement purposes:

- As required by law.
- In response to a court order, subpoena or other legal proceeding.
- To identify or locate a suspect, fugitive, material witness or missing person.
- When information is requested about an actual or suspected victim of a crime.
- To report a death as a result of possible criminal conduct.
- To investigate allegations of misconduct that may have occurred on our premises
- To report a crime in emergency circumstances.

Funeral Directors, Coroners and Medical Examiners – We may disclose protected personal information about you as necessary to allow these individuals to carry out their responsibilities.

National Security and Intelligence – We may disclose protected personal information about you to authorized federal officials for national security and intelligence activities.

Protective Services for the President and Others – We may use protected personal information about you to authorized federal officials for the provision of protective services to the President of the United

States or other foreign heads of state.

Uses or Disclosures That Require Your Authorization

Other uses and disclosures will be made only with your written authorization. You may cancel an authorization at any time by notifying our Complaint Officer in writing of your desire to cancel it. If you cancel an authorization it will not have any affect on information that we have already disclosed. Examples of uses or disclosures that may require your written authorization include the following:

- A request to provide your private personal information to an attorney for use in a civil law suit.

Your Rights

The information contained in your record maintained by the **AGENCY** are the physical property of the **AGENCY**. The information in it belongs to you. You have the following rights:

Right to Request Restrictions – You have the right to ask us not to use or disclose your private personal information for a particular reason related to our services or our operations. You may ask that family members or other authorized individuals not be informed of specific private personal information. That request must be made in writing to our Complaint Officer. We do not have to agree to your request. If we agree to your request, we must keep the agreement, except in the case of a medical emergency. Either you or the **AGENCY** can stop a restriction at any time.

Right to Inspect and Copy Your Protected Personal Information – You have the right to request to inspect and obtain a copy of your private personal information. You must submit your request in writing to our Complaint Officer. If you request a copy of the information or (IF YOU REQUEST) that we provide you with a summary of the information, we may charge a fee for the costs of copying, summarizing and/or mailing it to you.

If we agree to your request we will tell you. We may deny your request under certain limited circumstances. If your request is denied, we will let you know in writing and you may be able to request a review of our denial.

Right to Request Amendments to Your Protected Personal Information – You have the right to request that we correct your private personal information. If you believe that any private personal information in

your record is incorrect or that important information is missing, you must submit your request for an amendment in writing to our Complaint Officer.

We do not have to agree to your request. If we deny your request we will tell you why. You have the right to submit a statement disagreeing with our decision.

Right To An Accounting of Disclosures of Private Personal Information – You have the right to find out what disclosures of your private personal information have been made. The list of disclosures is called an accounting. The accounting may be for up to six (6) years prior to the date on which you request the accounting, but cannot include disclosures before July 1, 2004.

We are not required to include disclosures for services, payment or operations or for National Security or Intelligence purposes, or to correctional institutions and law enforcement officials. The right to have an accounting may be temporarily suspended if it will impede the agency's activities. The notice of suspension should specify the time for which such a suspension is required. Requests for an accounting of disclosures must be submitted in writing to our Complaint Officer. You are entitled to one free accounting in any twelve (12) month period. We may charge you for the cost of providing additional accountings.

Right To Obtain a Copy of the Notice – You have the right to request and get a paper copy of this notice and any revisions we make to the notice at any time.

Complaints

You have the right to complain to us and to the United States Secretary of Housing and Urban Development if you believe we have violated your privacy rights. There is no risk in filing a complaint.

If you are concerned that we may have violated your privacy rights, you disagree with a decision we made about access to your private personal information or in response to a request you made to amend or restrict the use or disclosure of your private personal information, or have us communicate with you by alternative means or at alternative locations, you may complain to us using the contact information listed in this notice.

To file a complaint with us, contact by phone or by mail:

Complaint Officer:

Questions and Information

If you have any questions or want more information about this Notice of Privacy Practices, please contact:

Brenda O'Connell, Lake County Planning Department

(847) 377-2331

By phone with questions or with written requests for information as defined under the **Your Rights** section of this notice. Complaints or questions may be made by phone or in writing.

We support your right to protect the privacy of medical information. We will not retaliate in any way if you choose to file a complaint with us.

Appendix C

Appendix D

Appendix E

Appendix F