Collier County Hunger & Homeless Coalition
Lead Agency
CRN Standard Operating Procedures
(Updated) November 27, 2019
V. 4.0

Exhibit I

Table of Contents

Section 5: Internal Operating Policies & Procedures (All included 45 CFR 164.308 (a)(5)(ii)))

05-010 System Availability Policies & Procedures
05-020 Technical Support Policies & Procedures

Section 6: Data Ownership, Usage & Release Policies & Procedures (Includes Sections: 06-010-020 45 CFR 164.310 (a)(2)(IV)

06-010 De-duplication Policies & Procedures
06-020 Data Quality Policies & Procedures
06-030 Data Ownership Policies & Procedures (Includes Sections: 06-030-060 45 CFR 164.308 (a)(3)(ii)(B))))
06-040 Data Classification Policies & Procedures
06-050 Data Uses & Disclosures Policies & Procedures
06-060 Data Release Policies & Procedures

Revisions control page

Date	Summary of changes made	Changes made by (Name)
4-3-17	Plan review	Michael Overway, CRN Administrator
10-10-18	Plan Review	Michael Overway, CRN Administrator
11-27-19	Plan Review	Michael Overway, ED and Nadja Joseph CRN Administrator

It is the intent of this manual to ensure the Collier County Continuum of Care FL 606 remains in compliance with 24 CFR HEARTH ACT, passed by Congress in 2009.

HUD Definitions per 24 CFR 576.2

576.2 Definitions.

Homeless means:

(1) An individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning:

(i) An individual or family with a primary nighttime residence that is a public or private place not designed for or ordinarily used as a regular sleeping accommodation for human beings, including a car, park, abandoned building, bus or train station, airport, or camping ground;

(ii) An individual or family living in a supervised publicly or privately operated shelter designated to provide temporary living arrangements (including congregate shelters, transitional housing, and hotels and motels paid for by charitable organizations or by federal, state, or local government programs for low-income individuals); or

(iii) An individual who is exiting an institution where he or she resided for 90 days or less and who resided in an emergency shelter or place not meant for human habitation immediately before entering that institution;

(2) An individual or family who will imminently lose their primary nighttime residence, provided that:

(i) The primary nighttime residence will be lost within 14 days of the date of application for homeless assistance;

(ii) No subsequent residence has been identified; and

(iii) The individual or family lacks the resources or support networks, ***e.g.,*** family, friends, faith-based or other social networks, needed to obtain other permanent housing;

(3) Unaccompanied youth under 25 years of age, or families with children and youth, who do not otherwise qualify as homeless under this definition, but who:

(i) Are defined as homeless under section 387 of the Runaway and Homeless Youth Act (42 U.S.C. 5732a), section 637 of the Head Start Act (42 U.S.C. 9832), section 41403 of the Violence Against Women Act of 1994 (42 U.S.C. 14043e-2), section 330(h) of the Public Health Service Act (42 U.S.C. 254b(h)), section 3 of the Food and Nutrition Act of 2008 (7 U.S.C. 2012), section 17(b) of the Child Nutrition Act of 1966 (42 U.S.C. 1786(b)) or section 725 of the McKinney-Vento Homeless Assistance Act (42 U.S.C. 11434a);

(ii) Have not had a lease, ownership interest, or occupancy agreement in permanent housing at any time during the 60 days immediately preceding the date of application for homeless assistance;

(iii) Have experienced persistent instability as measured by two moves or more during the 60-day period immediately preceding the date of applying for homeless assistance; and

(iv) Can be expected to continue in such status for an extended period of time because of chronic disabilities, chronic physical health or mental health conditions, substance addiction, histories of domestic violence or childhood abuse (including neglect), the presence of a child or youth with a disability, or two or more barriers to employment, which include the lack of a high school degree or General Education Development (GED), illiteracy, low English proficiency, a history of incarceration or detention for criminal activity, and a history of unstable employment; or

(4) Any individual or family who:

(i) Is fleeing, or is attempting to flee, domestic violence, dating violence, sexual assault, stalking, or other dangerous or life-threatening conditions that relate to violence against the individual or a family member, including a child, that has either taken place within the individual's or family's primary nighttime residence or has made the individual or family afraid to return to their primary nighttime residence;

(ii) Has no other residence; and

(iii) Lacks the resources or support networks, ***e.g.,*** family, friends, faith-based or other social networks, to obtain other permanent housing.

At risk of homelessness means: (1) An individual or family who:

(i) Has an annual income below 30 percent of median family income for the area, as determined by HUD;

(ii) Does not have sufficient resources or support networks, ***e.g.,*** family, friends, faith-based or other social networks, immediately available to prevent them from moving to an emergency shelter or another place described in paragraph (1) of the "homeless" definition in this section; and

(iii) Meets one of the following conditions:

(A) Has moved because of economic reasons two or more times during the 60 days immediately preceding the application for homelessness prevention assistance;

(B) Is living in the home of another because of economic hardship;

(C) Has been notified in writing that their right to occupy their current housing or living situation will be terminated within 21 days after the date of application for assistance;

(D) Lives in a hotel or motel and the cost of the hotel or motel stay is not paid by charitable organizations or by Federal, State, or local government programs for low-income individuals;

(E) Lives in a single-room occupancy or efficiency apartment unit in which there reside more than two persons or lives in a larger housing unit in which there reside more than 1.5 persons reside per room, as defined by the U.S. Census Bureau;

(F) Is exiting a publicly funded institution, or system of care (such as a health-care facility, a mental health facility, foster care or other youth facility, or correction program or institution); or

(G) Otherwise lives in housing that has characteristics associated with instability and an increased risk of homelessness, as identified in the recipient's approved consolidated plan;

(2) A child or youth who does not qualify as "homeless" under this section, but qualifies as "homeless" under section 387(3) of the Runaway and Homeless Youth Act (42 U.S.C. 5732a(3)), section 637(11) of the Head Start Act (42 U.S.C. 9832(11)), section 41403(6) of the Violence Against Women Act of 1994 (42 U.S.C. 14043e-2(6)), section 330(h)(5)(A) of the Public Health Service Act (42 U.S.C. 254b(h)(5)(A)), section 3(m) of the Food and Nutrition Act of 2008 (7 U.S.C. 2012(m)), or section 17(b)(15) of the Child Nutrition Act of 1966 (42 U.S.C. 1786(b)(15)); or

(3) A child or youth who does not qualify as "homeless" under this section, but qualifies as "homeless" under section 725(2) of the McKinney-Vento Homeless Assistance Act (42 U.S.C. 11434a(2)), and the parent(s) or guardian(s) of that child or youth if living with her or him.

Introduction – CRN Objectives

I. Introduction

The Collier County Community Resource Networks (CRN) is administered by the designated lead agency, The Collier County Hunger & Homeless Coalition, Inc. as the official Community Resource Network (CRN) of the Continuum of Care (CoC) of Collier County.

Purpose of this manual: This document sets forth the policies, procedures, guidelines, and standards that govern the CRN System. This manual also outlines the roles and responsibilities of Collier County Hunger & Homeless Coalition, which is the designated lead agency, and the participating partner agencies. All users of the CRN System agree to comply with the content of this manual and to comply with 24 CFR HEARTH ACT data collection. This manual is approved and amended periodically by the Board of Directors of Collier County Hunger & Homeless Coalition and CoC Board as deemed necessary.

Vision Statement:

CRN will improve the efficiency and effectiveness of services provided to those in the community who are homeless or at-risk of homelessness. Our approach will be collaborative and client-centered, focused on improving the health, recovery, safety, quality of care and, ultimately, the self-sufficiency of clients.

CRN will follow best practices for data sharing and outcome measurements to provide accountability to all community partners while respecting client and service provider confidentiality.

Method:

- Collier County Hunger & Homeless Coalition is responsible for the basic architecture, including staff training, support and overall coordination with the software vendor and ensuring compliance with applicable confidentiality law and governing standards.

- Web-based database management provides client tracking, case management, service and referral management, bed availability for shelters, resource indexing, and reporting. The software vendor is Bowman Systems.

- Minimum hardware standards provide networking capabilities for data sharing and communication among participating agencies.

- The focus of this system implementation is tracking homeless individuals, although agencies will be able to utilize it for all services provided.

Benefits for persons who are homeless: The CRN system will increase the responsiveness and effectiveness of services for people who are homeless. Homeless persons will not need to repeat their demographics, history and needs at each service location. Case managers will be able to see services available to clients and individuals can be further tracked for successful completion of goals. The communication made possible by the system will increase the extent to which service providers can meet the needs of the person seeking assistance.

Benefits for service providers: Case managers and other service provider staff will use the CRN to assess their clients' needs, inform clients about resources, and coordinate service provision both within and between service agencies. The system will be a tool to enhance communication, coordination, and assistance in setting and achieving goals. Further, aggregated information will be used to advocate for additional resources, complete grant applications, conduct evaluations of the programs and delivery systems, and to provide reports for funding agencies.

Benefits for the community and policy makers: The aggregated data resulting from the CRN System will help inform policy decision makers that will affect the homeless in our community. The community and its decision makers will have data available to help better understand the causes of homelessness, current trends, program effectiveness, and gaps in existing systems.

II. **General Principles for all Participants**

a. **Integrity**: Information solicited for input in the CRN should be done so in a manner that preserves the integrity of the database. Only information that has been confirmed to be true and accurate is to be entered into the system.

b. **Privacy**: Information solicited for input in the CRN should be done so in a manner that preserves the privacy of the individual giving the information. All system users are required to adhere to all applicable federal and state laws regarding privacy and confidentiality.

c. **Client Self-determination**: When soliciting information for the CRN, users must remember that the client has the unconditional right to determine the services that they desire to participate in, regardless of professional opinion. It is our desire to work in tandem with clients, forming a partnership with the shared goal of assisting our clients.

d. **Respect**: Services provided to clients in the Continuum of Care should be done so in a manner that preserves their respect.

e. **Dignity**: Services provided to clients in the Continuum of Care should be done so in a manner that preserves their dignity.

Section 1 – Contractual Responsibilities

SOP#: 01-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN LEAD AGENCY RESPONSIBILITIES		

Policy: A lead agency will be assigned and have the responsibilities stated below.

Standard: The related responsibility for the lead agency will be apportioned per the information provided below.

Purpose: To define the roles and responsibilities of the lead agency with respect to CRN/CRN activities.

Scope: Continuum of Care / CRN Lead Agency.

Designation: The lead agency for the CRN is Collier County Hunger & Homeless Coalition.

Responsibilities:

- Employment of the Project Manager/System Administrator whose roles are described in SOP# 01– 030;
- Obtain hosting services and purchases contract with software vendor(s);
- Maintain adequate property and liability insurance coverage provided through the funding associated with CRN. At present this includes equipment, software, and connectivity directly related to the day-to-day operation of the Project Management & System Administrator office;
- Secure funding and funding policies in coordination with the recognized lead agency for Collier County Continuum of Care, which is Collier County Hunger & Homeless Coalition; and
- Coordinate community participation.
- Compliance with 24 CFR HEARTH ACT and revised HUD Data Standards as of August 2016.

SOP#: 01-020
Approval Date: Pending Revision Date: Revised by:
Title: CRN STEERING COMMITTEE RESPONSIBILITIES

Policy: The CRN Steering Committee will approve all major CRN/CRN policy decision makers for recommendation to the Board of Directors of the CRN Lead Agency.

Standard: The CRN/CRN related responsibilities of the CRN Steering Committee will be apportioned per the information provided below.

Purpose: To define the roles and responsibilities of the CRN Steering Committee with respect to CRN/CRN activities.

Scope: Continuum of Care

Responsibilities:

The CRN Steering Committee will support the overall CRN/CRN initiative, advising the CRN Management on CRN/CRN operations. The CRN Steering Committee shall meet at least quarterly, at which time CRN decision points can be raised for discussion and/or approval. The CRN Steering Committee shall designate a committee or task group to develop and help enforce the implementation of CRN policies.

The CRN Steering Committee's role is fundamentally advisory to the CRN/CRN project overall. However, the CRN Steering Committee has authority to approve final decisions on the selected key issues that follow.

These issues include:

- Determining the guiding principles that shall underlie the CRN/CRN implementation activities of the CRN participating organizations and service programs;
- Setting and enforcing minimum data collection requirements, as defined in SOP# 03-070: Data Collection Requirements;
- Encouraging Continuum of Care-wide provider participation;
- Facilitating client involvement;
- Defining privacy protection and confidentiality policies for all CRN/CRN activities;
- Defining criteria, standards, and parameters for the usage and release of all data collected as part of the CRN; and
- Compiling and analyzing CRN data with other provider and community data sources.

SOP#: 01-030 Revision: Prepared by: CRN
Approval Date: Pending Revision Date: Revised by:

Title: CRN PROJECT MANAGER/SYSTEM ADMINISTRATOR RESPONSIBILITIES

Policy: A Project Management structure will be put into place to adequately support the operations of the CRN per the policies and procedures described in this document.

Standard: The responsibilities of the CRN Project Manager/System Administrator will be apportioned per the information provided below.

Purpose: To define the roles and responsibilities of the CRN Project Manager/System Administrator.

Scope: The CRN Project Manager/System Administrator.

Responsibilities:

The CRN Project Manager/System Administrator is responsible for:

- Oversight of the Partner Agencies' adherence to the CRN policies and procedures, as determined by the CRN Steering Committee;
- Creation of an annual budget and project specific budgets for the lead agency's approval; and
- Supervision of the contractual relationships with vendors.

The CRN Project Manager/System Administrator is also responsible for oversight of all day-to-day operations including:

- Quality assurance of the vendor application operation;
- Managing agency and user system access based on execution of applicable agreements, training, and adherence to approved policies;
- Providing technical support and application training to users, in compliance with levels documented in SOP# 05-020: Technical Support Policies and Procedures;
- Developing a reasonable number of reports for CRN users based on requests from the CRN Steering Committee or its designated committee;
- Maintaining overall CRN quality assurance program;
- Orientation and supervision of CRN software and hosting vendor to ensure appropriate program operations and compliance with guiding principles and Standard Operating Procedures.
- Understanding all aspects of the vendor CRN product (commonly referred to as the CRN);
- Provision of ad-hoc application training and technical support to users, overall functionality, and agency-level system administration functionality;
- Communicating system availability, planned and unplanned outages, and other CRN information to Agency Super User;

- Assigning user IDs to new users based on the approved licensing structure, authorized agency requests, and documentation of user training;
- Managing user accounts and application access control, in conjunction with the Agency Super User and hosting company;
- Managing data sharing configuration, based on submission of executed Interagency Data Sharing Agreements;
- Assisting with agency data migration;
- Supervision of CRN Database Administration as part of the contractual oversight of hosting and software vendor;
- Recommending the creation and modification code definitions & business rules as well as application level changes to set-ups and configurations to the appropriate vendor;
- Designing management, program, analytical and agency level reports per predefined CRN standard formats and/or funding requirements or as requested by the CRN Lead Agency;
- Designing and managing report structure, library and archive in cooperation with the software vendor;
- Managing report access control; and
- Communicating significant application issues and/or system enhancement requests to the software vendor and governing bodies.

The CRN Project Manager/System Administrator will respect the core principles of the system by:

- Ensuring with the software vendor that access to areas containing equipment, data, and software will be secured in accordance with HUD Data and Technical Standards;
- Strictly safeguarding all client-identifying information in accordance with all applicable HUD Data and Technical Standards, Federal and State laws using the latest technology available;
- Securely protecting all data to the maximum extent possible; and
- Conducting ongoing security assessments to include penetration testing on a regular basis.

SOP#: 01-040	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN USER GROUP RESPONSIBILITIES		

Policy: The Partner Agencies shall have a forum for providing input on planning and CRN governance issues.

Standard: All Agency End Users and Agency Super Users will serve on the CRN User Group to formally manage communication between user agencies and CRN Project Manager/System Administrator on all system issues.

Purpose: To outline the major responsibilities of the CRN User Group.

Scope: System-wide

Responsibilities:

The CRN User Group is responsible for:

- Identifying and prioritizing system enhancements;
- Identifying and recommending solutions for known problems to the Project Manager;
- Providing quick feedback loop on system performance; and
- Providing recommendation for training and best practices for CRN.

User Group Chair/Co-chairs may be involved in the process of imposing sanctions on users/agencies for misuse of system. (This procedure is further specified in SOP 04-030: Auditing Policies and Procedures.)

SOP#: 01-050	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN AGENCY EXECUTIVE DIRECTOR RESPONSIBILITIES

Policy: The Executive Director of each Partner Agency will be responsible for oversight of all agency staff members who generate or have access to client-level data stored in the system software to ensure adherence to the CRN standard operating procedures outlined in this document.

Standard: The Executive Director of each Partner Agency holds final responsibility for the adherence of his/her agency's personnel to the CRN guiding principles and Standard Operating Procedures outlined in this document.

Purpose: To outline the role of the agency Executive Director with respect to oversight of agency personnel in the protection of client data within the CRN application. Throughout this manual, the use of the title Executive Director indicates the Executive Director of the agency or the person in that agency holding the title equivalent to Executive Director.

Scope: Executive Director or equivalent in each Partner Agency

Responsibilities:

The Partner Agency's Executive Director is responsible for all activity associated with agency staff access and use of the CRN. This person is responsible for establishing and monitoring agency procedures that meet the criteria for access to the CRN, as detailed in the Standard Operating Procedures (SOPs) outlined in this document. The agency's Executive Director will be ultimately responsible for any misuse of the software system at their agency. The agency's Executive Director agrees to only allow access to the CRN based upon need. Need exists only for those program staff, volunteers, or designated personnel who work directly with, or supervise staff who work directly with, clients or have data entry or other data-related agency administrative responsibilities.

The **Executive Director** as designated by each participating agency will be responsible for oversight of all agency staff that generate or have access to client-level data stored in the system software to ensure adherence to the CRN Policies and Procedures and all government regulations.

The Partner Agency's Executive Director also oversees the implementation of data security policies and standards and will:

- Assume responsibility for completeness, accuracy, and protection of client-level data entered into the CRN system;

- Establish business controls and practices to ensure organizational adherence to the CRN SOPs;

- Assign an agency Super User to manage agency-related technical tasks whose role is described in SOP# 01-060;
- Communicate control and protection requirements to agency custodians and users;
- Authorize data access to agency staff and assign responsibility for custody of the data;
- Monitor compliance and periodically review control decisions;
- Implement adequate agency policies and procedures to safeguard the confidentiality and security of data in accordance with all HUD Data and Technical Standards and all applicable laws and regulations;
- Require Agency Super Users and End Users to participate in CRN training;
- Require Agency Super User and End Users to participate in User Group meetings;
- Maintain adequate property liability insurance coverage to safeguard hardware acquired with CRN from possible client claims associated with CRN use;
- Properly maintain all components of the hardware acquired with CRN funding, and report to the CRN Project Manager relevant changes in the equipment status;
- Maintain a complete inventory list including product and serial number. Each article or component shall be tagged with an inventory number and the manufacturer's serial number, where applicable; and

SOP#: 01-060	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN AGENCY SUPER USER RESPONSIBILITIES		

Policy: Every Partner Agency must designate one person to be the Agency Super User.

Standard: The designated Agency Super User holds responsibility for the administration of the system software in his/her agency.

Purpose: To outline the role of the Agency Super User

Scope: Partner Agencies

Responsibilities:
The Executive Director of each Partner Agency will appoint a qualified person as the agency Super User, who will need to successfully complete the Technical Administration training provided by Project Manager/System Administrator.

This person will:

- Coordinate with the agency Executive Director for the proper use of the CRN within the participating agency, including adherence to all CRN policies and procedures;
- Provides and coordinates training and technical support to end users within the agency and with the Project Manager/System Administrator;
- Ensure that access to the CRN be granted to staff/volunteers only after they have received training and demonstrated proficiency in the use of the software, along with an understanding of policies and procedures related to CRN;
- Ensure that Agency End User IDs are not shared beyond the authorized staff person;
- Seek assistance from the CRN Project Manager/System Administrator as needed;
- Communicate regularly with the CRN Project Manager/System Administrator to ensure the integrity of the CRN;
- Participate in scheduled CRN User Group Meetings;
- Maintain the participating agency's list of end user IDs and associated names;
- Immediately inform the CRN Project Manager/System Administrator of any breaches in security or confidentiality;
- Ensure that CRN forms are utilized properly and in compliance with CRN policies and procedures;
- Be responsible for conveying to Agency End Users and clients the spirit of protecting client data confidentiality and security;
- Be aware of and uphold all state and federal regulations regarding client confidentiality and their rights to privacy;
- Provide updates to CRN to reflect changing information about the Participating Agency;

- Ensure information is being entered and is as complete as appropriate;
- Determine security level of staff; and
- Define any agency specific data that is needed.
- Enter data as required by 24 CFR HEARTH ACT, CRN Data Standards August 2016 for reporting to the Dept. of HUD and Florida Dept. of Children & Families (DCF).

SOP#: 01-070	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN AGENCY END USER RESPONSIBILITIES		

Policy: Only trained Agency End Users who have signed a User's Agreement will have access to the CRN.

Standard: The related responsibility for the Agency End User will be apportioned per the information provided below.

Purpose: To define the roles and responsibilities of the Agency End User.

Scope: Participating Agency

Every End User in the agency will:

- Abide by the policies and procedures of the CRN, with special emphasis on confidentiality and security issues;
- Abide by the Participating Agency's internal policies and procedures;
- Fully and accurately communicate both orally and in writing (or some other means if a disability or other reason prevents a client from comprehending oral and written information) the rights of those clients with respect to their consent and authorization for data input, interagency information sharing, and aggregate reporting;
- Participate in system training and in scheduled CRN User Group Meetings;
- Enter all information in a manner appropriate for your agency and the community CoC universal required data elements
    - Entry records using the Coordinated Intake Assessment must be filled in at intake – each section header and subsequent questions must be completed for each intake performed within 24 hours of program contact unless over a weekend, do not update another agencies assessment,
    - Exit Assessment is used when exiting a client from program – all questions must be answered;
- Make sure all data collection follows 24 CFR HEARTH ACT data collection regulations as amended in August 2016– CRN HEARTH Regulations will be updated periodically – when issued Collier CRN will notify the agency;
- Be aware of and uphold all CRN Privacy & Security Policy including state and federal regulations regarding client confidentiality and their rights to privacy.

Section 2 – Implementation Policies & Procedures

SOP#: 02-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN PARTICIPATION POLICY		

Policy: Agencies that are funded through Continuum of Care Committee efforts for services to the homeless in Collier County will be required to participate in the CRN. All other agencies serving the homeless and clients at-risk of homelessness are strongly encouraged to participate in the CRN.

Standard: Lead Agency will provide quality CRN services to all participating agencies through CRN.

Purpose: To outline which agencies are expected to participate in the CRN, the extent to which their participation is mandatory or voluntary, and a definition of participation.

Scope: All at risk and homeless providers

Procedure:

Beginning with 2003 CoC and ESG grants, HUD is requiring all grantees and sub-recipients of McKinney-Vento and homeless HOPWA grants to participate in the local CRN. McKinney-Vento grants include Emergency Shelter Grants and Supportive Housing Program, Section 8 Moderate Rehabilitation SRO, and Shelter Plus Care (now HUD Rental Assistance) grants. This policy is consistent with the Congressional direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness. The CRN and its operating policies and procedures are structured to comply with the HUD Data and Technical Standards Final Notice as amended August 2016. It is recognized that agencies may be further regulated by HIPAA and other Federal, State and local laws. Therefore, the CRN Lead Agency may negotiate its procedures and/or execute appropriate business agreements with partner agencies so they are following applicable laws. This policy applies to; non-profit, for profit, faith-based, and government agencies utilizing the CRN.

Participation Requirements

Mandated Participation

All providers that are funded by the Continuum of Care to provide homeless services must meet the **Minimum Participation Standards** of the CRN, as defined by this SOP. Participating agencies will be required to comply with all applicable SOPs, and must agree to, execute, and comply with a CRN Agency Partner Agreement. Updated, modified and custom agreements may be developed to accommodate additional CRN Partner Agencies who already have their own client management system.

Voluntary Participation

Although mandated agencies are required to meet minimum participation standards, the CRN Lead Agency strongly encourages mandated agencies to fully participate with all their relevant homeless programs and supportive services to at risk populations.

While the CRN Lead Agency cannot require non-funded providers to participate in the CRN, they will work closely with non-funded agencies to articulate the benefits of the CRN and to strongly encourage their participation to achieve a comprehensive and accurate understanding of homelessness in Collier County.

Minimum Participation Standards for Mandated and Voluntary Participants.

Each agency will have an opportunity to determine which participation option is most appropriate given agency functional and administrative needs, technological capacity, funding requirements, client characteristics and circumstances, and legal constraints. Agencies that receive funding from the Continuum of Care must meet specific funding requirements related to data submittal.

Domestic Violence providers that receive McKinney-Vento funding will be required to participate using the Direct Partner (or Interface Partner) options (CRN Agency Partner Agreement) for the McKinney-Vento funded programs, based on the participation requirements specified in the 2016 HUD Data and Technical Standards Final Notice. CoC Compliance to 24 CFR HEARTH ACT is required as CRN Standards are released from HUD.

The participation options are described below. If additional information is desired, CRN Lead Agency management can elaborate on each option to help each partner agency decide on the most appropriate way of participating in the Continuum's CRN initiative.
Minimal participation includes:

-Collecting the universal data elements, as defined in SOP# 03-070: Data Collection Requirements, for all programs operated by the agency that primarily serve persons who are homeless or formerly homeless or at risk of homelessness including the HUD 40118 assessment.

-Collecting program-specific data elements, as defined in SOP# 03-070: Data Collection Requirements, for all clients served by a program funded by the Continuum of Care.

-Submitting data to the CRN Lead Agency using one of the following options:

- **Direct Data Entry Option*:*** Entering client-level data into the CRN, defined as Direct Partner. (Agency Partner Agreement).
  The CRN central database server is protected by numerous technologies to prevent access from unauthorized users. Unless a client requests that his/her identifiers remain hidden at the time that his/her record is created, primary client identifiers (e.g. name, SSN, DOB and gender) will be able to be queried by other CRN users to prevent duplicate records from being created in the database. However, other individual client data will not be accessible by other CRN users outside of the client notification and interagency data sharing procedures. These procedures are described in SOP# 03-060: Client Notification Policies and Procedures and SOP# 03-080: Interagency Data Sharing for compliance with 24 CFR HEARTH ACT.

Anonymous CRN Data Submittal Option: Due to legal constraints, extreme vulnerability, and heightened safety needs of victims of domestic violence, DV providers have the option of submitting anonymous client-level data for programs that are not funded with HUD McKinney-Vento. (Anonymous CRN Data Submittal Partner Agency). If a DV agency determines that it cannot participate using any of the above options based on legal constraints, and the vulnerability and safety needs of its clients, the agency can participate by submitting anonymous client-level data about the persons served by their program. This data will be collected and analyzed by the CRN Lead Agency as part of its effort to understand homelessness and system effectiveness in the County. Anonymous, client-level data will be merged into the CRN Lead Agency analytical database with de-identified, unduplicated client-level data from other service providers. SOP# 03-070: Data Collection Requirements defines which data elements are considered client personal identifying information, and which will not be required for submittal to ensure an unduplicated count across the Continuum of Care.

All submitted data will be used by the CRN Lead Agency for analytical and administrative purposes, including the preparation of reports to funders and stakeholders. A client has the right to refuse to have his/her data entered into the CRN database. The client's individual choice regarding participation will not affect his/her right to services. All data should be submitted on a quarterly basis. See SOP# 03-050.

SOP#: 02-020	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN INITIAL PARTICIPATION REQUIREMENTS

Policy: Each Partner Agency must meet all initial participation requirements to receive access to the CRN.

Standard: CRN Project Manager /System Administrator will certify that the Partner Agency has met the participation requirements prior to initiating the CRN.

Purpose: To provide agencies with clear expectations for their participation in the CRN.

Scope: System-wide

Requirements:

CRN Group Orientation and a One-on-One Agency Meeting: Agency representatives are required to participate in a CRN Group Orientation and a one- on- one Agency Meeting to discuss CRN goals and objectives, requirements, site considerations, and documentation. A completed Agency CRN Implementation Requirements Checklist must be present in the CRN Project Manager's agency file prior to CRN access.

Partner Agreement: An authorized agency representative is required to execute a Partner Agreement stating his/her commitment to uphold the policies and procedures for effective use of the system and proper collaboration with the CRN Project Management/System Administrator. An executed Agency Partner Agreement must be present in the CRN Project Manager's Agency file prior to CRN access.

Information Security Protocol: Documentation of the agency's Information Security Protocol (developed in accordance with SOP# 02-030: CRN Agency Information Security Protocol Requirements) and dissemination plan must be on-site at agency prior to CRN access.

Documentation: All documentation on agency and program information must be submitted to ensure that complete and accurate Partner Agency information is input within the CRN. All intake forms and necessary reports must be present in the CRN Project Manager's agency file and agency specific system configuration must be completed and successfully tested prior to CRN access.

Agency Super User: One key staff person or contractor must be designated to serve as the Agency Super User. (See SOP# 01-060) The Agency Super User must be formally identified and attend Agency Super User Training prior to CRN access.

Site Hardware & Connectivity Requirement: Any computer being used to access the CRN must meet the minimum hardware and recommended connectivity requirements indicated in SOP# 02-040: CRN Agency Hardware and Connectivity Requirements.

Fees: All applicable fees must be paid as part of the implementation. (**In the event CRN institutes a fee schedule**.)

- Each Partner Agency will be assigned a specified number of user licenses that will be fully subsidized by the CCHC as part of the CRN initiative, including user related hosting and support costs, provided sufficient funding is available.

- The CRN Lead Agency will subsidize overhead, training, and technical support costs associated with CRN policy and software training, such as staff, location, curriculum development, and web-enabled technical support materials.

- For agencies implementing in 2016-2017, all training costs will be fully subsidized by the CRN Lead Agency. Beyond 2017, agencies may be asked to pay a training fee per user/agency to cover training expenses, such as but not limited to, printed materials, refreshments.

Data Migration: All data that will be migrated from a Direct Partner Agency's existing database to the CRN database must be cleaned, updated, and formatted per CRN data specifications prior to migration. The specific conversion process must be individually discussed with the CRN Project Manager/System Administrator.

SOP#: 02-030	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN AGENCY INFORMATION SECURITY PROTOCOL REQUIREMENTS

Policy: Partner Agencies must develop and have in place minimum information security protocols to protect client information stored in the CRN database.

Standard: CRN Project Manager/System Administrator will certify that the Partner Agency has adequate documentation of its information security protocol, a dissemination plan, and verification that the information security protocols have been implemented within the agency prior to granting CRN access.

Purpose: To protect the confidentiality of client data and to ensure its integrity at the agency site.

Scope: Direct Partner Agencies

Requirements:

At a minimum, the Direct Partner Agency must develop rules, protocols or procedures that are consistent with Section 3: Operational Policies and Procedures and Section 4: Security Policies and Procedures to address the following:

- Internal agency procedures for complying with the CRN Notice of Uses and Disclosures and provisions of other CRN client and agency agreements (See SOP# 03-060: CRN Client Notification and Consent Procedures);
- Maintenance of an updated copy of the agency's Notice of Uses and Disclosures or equivalent privacy notice on the agency's website, in accordance with SOP# 03-060.
- Appropriate assignment of user accounts;
- Prevention of user account sharing;
- Protection of unattended workstations;
- Protection of physical access to workstations where employees are accessing CRN;
- Safe storage and protected access to hardcopy and digital CRN generated client records and reports with identifiable client information;
- Proper cleansing of equipment prior to transfer or disposal; and
- Procedures for regularly auditing compliance with the Agency Information Security Protocol.

SOP#: 02-040	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN AGENCY HARDWARE, CONNECTIVITY AND SECURITY REQUIREMENTS

Policy: Any computer that interfaces with the CRN must meet the minimum desktop specifications and recommended connectivity specifications identified by this SOP.

Standard: The Partner Agency must certify that they have adequate hardware and connectivity to interface with the CRN prior to granting CRN access.

Purpose: To provide agencies with minimum requirements for hardware and connectivity.

Scope: System-wide

Requirements:

Workstation Specifications:

Computers interfacing with CRN must meet the minimum desktop specifications below.

- Operating System: Windows 7 or newer with Service Pack
- Processor: 2 GB Pentium processor or higher
- Memory: 512 MB RAM
- Video: Color monitor (22" Recommended) with graphics card that supports 1024 x 768-display resolution, 256 Colors or better.
- Web Browser: MS Internet Explorer 11, Service Pack 2 / MS Internet Explorer 7 / or MS Internet Explorer 11.01, Service Pack 1, Mozilla 3+, or Google Chrome

Internet Specifications:

Agencies directly entering data must have internet connectivity for each workstation that will be accessing the CRN. All agencies must have high speed internet connection with a cable modem or DSL/ISDN or faster. Service Point utilizes a commercial grade 128-bit encryption by VeriSign secured log in process.

Security Specifications:

All workstations accessing the CRN must have:

- Adequate firewall protection and apply all critical virus and system updates automatically; and
- Virus protection software. Virus definitions must be updated automatically.

SOP#: 02-050	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN USER IMPLEMENTATION REQUIREMENTS

Policy: All Partner Agency users and the CRN Project Manager/System Administrator who require legitimate access to the software system will be granted such access only upon completion of required training and execution of a CRN User Agreement.

Standard: Individuals with specific authorization to access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

Purpose: To outline the role and responsibilities of CRN users.

Scope: System-wide

Responsibilities:

Eligible Users

The CRN Project Manager/System Administrator shall only authorize use of the CRN to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out central server responsibilities.

The Partner Agency shall only authorize use of the CRN to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

User types are defined in SOP# 03-030: CRN User Access Levels.

User Requirements

Prior to being granted a username and password, users must:

- Execute an CRN User Agreement; and
- Successfully complete all CRN policy and application training required for assigned user level. (Training requirements are documented in SOP# 03-040: CRN Training Requirements.)

CRN users cannot attend training until all agency and user paperwork is completed and approved by the Executive Director (or authorized designee). Users must be aware of the sensitivity of client-level data and take appropriate measures to prevent unauthorized disclosure of it. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with all policy and standards described in these Standard Operating Procedures. They are accountable for their actions and for any actions undertaken with their usernames and passwords.

Enforcement Mechanisms

All potential violations of any security protocols will be investigated by CRN Project Manager/System Administrator. Any user found to be in violation of security protocols will be sanctioned per the procedure delineated in SOP# 04-030: Auditing Policies and Procedures. Sanctions include, but are not limited to:

- a formal letter of reprimand;
- suspension of system privileges;
- revocation of system privileges; and

A Partner Agency's access may also be suspended or revoked if serious or repeated violation(s) of the SOPs occur by Agency users.

Section 3 – Operational Policies & Procedures

SOP#: 03-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN AGENCY SET-UP PROCEDURE

Policy: The CRN Project Manager/System Administrator may set up a new agency account, based on the following procedure.

Standard: The CRN Project Manager/System Administrator must verify documentation of all initial implementation requirements listed in Section 2 prior to authorizing a new agency.

Purpose: To inform potential agencies and the CRN Project Manager/System Administrator of the Agency set-up requirements.

Scope: Direct Partner Agencies and Interface Agencies

Responsibilities:

Prior to setting up a new Direct Partner Agency within the CRN database, the Executive Director of the proposed agency must ensure completion of the required implementation requirements outlined in Section 2: Implementation Policies and Procedures.

The CRN Project Manager/System Administrator shall:

- Review CRN records to ensure that the Agency does not have previous violations with the CRN SOPs that prohibit access to the CRN;
- Verify that the required documentation has been correctly executed and submitted, including:
  - Initial Implementation Requirements Checklist;
  - Executed Agency Partner Agreement;
  - Agency, User, and Program Information Forms;
  - Designation of Agency Super User;
- Request and receive approval from the CRN Lead Agency to set up a new agency;
- Authorize a new Agency within the CRN;
- Work with the Agency Super User to input applicable agency and program information; and
- Work with Agency Super User to migrate legacy data, if applicable.

The process for setting up Interface Agencies is comparable, except that the CRN Project Manager/System Administrator must also work with agencies to develop an approved interface to upload data from the agency database to the CRN database.

SOP#: 03-020	Revision:	Prepared by: CRN
Approval Date: 01/04/2005	Revision Date:	Revised by:

Title: CRN USER SET-UP PROCEDURE

Policy: The CRN Project Manager/System Administrator may create a new User ID for eligible individuals based on the following procedure.

Standard: The CRN Project Manager/System Administrator must document that the following set-up procedure has occurred prior to setting up a new user.

Purpose: To inform all parties involved with the CRN of the requirements to become an CRN user.

Scope: Direct Partner Agencies and Interface Partner Agencies

Responsibilities:

If the Direct Partner Agency wants to authorize system use for a new user, the agency Executive Director (or authorized designee) must:

- Determine the access level of the proposed CRN user (See SOP# 03-030 CRN User Access Levels); and
- Authorize the creation of a user account for the specified individual by completing a New User Request form that designates the access level.

The proposed CRN user must:

- Attend applicable training modules (once enrolled by the Agency Super User); and
- Execute a CRN User Agreement.

The Agency Super User must:

- Input the user information into an 'CRN New User Request' form for CRN Project Manager/System Administrator approval;
- Enroll the potential CRN user in the required training modules; and
- Submit the executed CRN User Agreement as an original to the CRN Project Manager/System Administrator.

The CRN Project Manager/System Administrator shall:

- Review CRN user records to ensure that a user does not have previous violations with the CRN SOPs that prohibit access to the CRN;

- Verify that the required documentation (CRN New User Request form and CRN User Agreement) have been correctly executed and submitted;
- Verify that required training modules have been successfully completed; and
- Approve the new user request by assigning a user ID and password.

SOP#: 03-020 Title: CRN USER SET-UP PROCEDURE

Once the user ID is established, the CRN Project Manager/System Administrator is responsible for maintaining the user account. The Agency Super User is also responsible for immediately informing the CRN Project Manager/System Administrator if any user terminates employment with the agency, or otherwise no longer needs access to the CRN.

The Executive Director is responsible for ensuring that the user understands and complies with all applicable CRN SOPs.

SOP#: 03-030	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN USER ACCESS LEVELS

Policy: Each CRN user shall be assigned a designated user access level that controls the level and type of access the individual has within the system.

Standard: The CRN System Administrator will not issue a user ID until the agency Executive Director (or authorized designee) has submitted a New User Request form that designates the access level.

Purpose: To designate CRN user access levels.

Scope: Direct Partner Agencies and Interface Partner Agencies

Responsibilities:

All CRN users must be assigned a designated user access level that controls the level and type of access that user has within the system. Unless otherwise specified below, each user will only have access to client-level data that is collected by their own agency or an agency network partner, unless a client specifically consents to temporary information sharing for referral purposes.

(See table next page)

SOP#: 03-030 Title: CRN USER ACCESS LEVELS

The level of access for each CRN user type is defined in the table below.

USER TYPES	Intake (Identifiers)*; Family Relationships: Housing History*	Income & Benefits History; Public Assistance History; Educational and Vocational History; Employment History*; Veteran Information	Legal Information; Basic Medical Information	Special Needs Screening	Clinical Mental Health Assessment Clinical Substance Abuse Information, Clinical HIV/AIDS Information	DV Incident Tracking	Program Registration; Program Exit; Service Plans; Services Received; Referrals	Case Notes	Bed Management (Availability)	Bed Management (Bed Assignment)	Information & Referral System	Agency Admin. Functions**	Reports (De-identified)	Reports (Identified)
Agency Initial User	V						V		V		V			
Agency End User	M	A					A	A	V	A	A			
Agency ED/CEO	V	V	V	V	V	V	V	V	V	V	V		V	V
Agency End User	M	M	M	M	M	M	M	A	M	M	V		V	V
Agency Super User	M	M	M	M	M	M	M	D	D	D	M	Y	V	V
CRN PM & SA	D	D	D	D	D	D	D	D	D	D	D	Y	C	C
Coalition ED									V		V		V	V

Legend:

V = View Only
M = View, Add and Modify
C = Create Reports
D = Delete Entries
A = View and Add New Data
Y = Access to execute specified functions

SOP#: 03-040	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN USER TRAINING REQUIREMENTS

Policy: CRN users shall successfully complete the training modules required for their user type.

Standard: The CRN System Administrator will not issue a user ID until documentation of successful completion of required training is provided.

Purpose: To inform users of the training requirements to access the CRN.

Scope: Direct Partner Agencies and Interface Partner Agencies

Responsibilities:

Prior to gaining access to the CRN application, users must successfully complete the following training modules.

User Type	Training Module(s)	Training Provider
Coalition ED	Basic Computer Training (optional, based on users' computer skills) Basic CRN Policy Training for Agency Users Basic CRN Application Training for Report Viewing	Community Resources (see referral list) CRN Project Manager & System Administrator
Agency Initial User	Basic Computer Training (optional, based on users' computer skills) Basic CRN Policy Training for Agency Users Basic CRN Application Training for Agency Users	Community Resources (see referral list) CRN Project Manager & System Administrator
Agency ED	Basic Computer Training (optional, based on users' computer skills) Basic CRN Policy Training for Agency Users Basic CRN Application Training for Agency Users	Community Resources (see referral list) CRN Project Manager & System Administrator

User Type	**Training Module(s)**	**Training Provider**
Agency End User	Basic Computer Training (optional, based on users' computer skills) Basic CRN Policy Training for Agency Policy Users Basic CRN Application Training for Agency Policy User	Community Resources (see referral list) CRN Project Manager & System Administrator
Agency Super User	Basic CRN Policy Training for Agency Technical Administrators Basic CRN Application Training for Agency Users Advanced CRN Application Training on Agency Technical Administration	 CRN Project Manager & System Administrator
CRN Project Manager & System Administrator	Advanced CRN Application Training on Overall Technical Administration	Community Resources Software Vendor

SOP#: 03-050	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN CLIENT SET-UP PROCEDURE

Policy: Each user must follow the client set-up procedure when creating a new client record.

Standard: The Executive Director of each Partner Agency must ensure that the agency has adequate procedures in place to ensure that client records are set up per this procedure.

Purpose: To inform agencies and users about the appropriate client setup procedures.

Scope: System-wide

Responsibilities:

For Direct Partner Agencies:

1) Explain CRN to client, per SOP# 03-060: CRN Client Notification Procedure;
2) Search for existing Client Record. Select existing client record or create a new client record;
3) Collect client information per SOP# 03-070: CRN Data Collection Requirements; and
4) If appropriate, grant inter-agency sharing, per SOP# 03-080: CRN Interagency Data Sharing Procedures.

For Interface Partner Agencies:

1) Ensure that agency database generates unduplicated client analysis;
2) Explain Agency's intent to share client information with the CRN, per SOP# 03-060: CRN Client Notification Procedure;
3) Collect client information, per SOP# 03-070: CRN Data Collection Requirements; and
4) Upload client information on a weekly, if not more frequent, basis.

For Anonymous CRN Data Submittal Partner Agency

1) Ensure that agency database generates unduplicated client analysis;
2) Collect client information, per SOP# 03-070: CRN Data Collection Requirements; and
3) Submit anonymous client-level data to the CRN Database on a quarterly basis.

SOP#: 03-060	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN CLIENT NOTIFICATION POLICIES AND PROCEDURES

Policy: Partner Agencies shall use the required client notification and consent procedure prior to entering any client-level data into the CRN.

Standard: The Executive Director of each Partner Agency is responsible for ensuring that the agency has implemented appropriate procedures to enforce the client notification and consent procedures, consistent with HUD CRN Data & Technical Standards, and applicable state and federal laws and rules regarding client confidentiality and consent.

Purpose: To give clients control of their personal information.

Scope: System-wide

Responsibilities:

All verbal and written client notification and consent must include a statement that no client will be denied service for refusal to consent. The CRN Steering Committee has prepared standard documents for Client Notice of Uses and Disclosures, Client Consent for Network Data Sharing, and Client Release of Information for Agency Referrals. Partner Agencies may either use these forms or incorporate the content of the CRN documents in their entirety into the Agency's own documentation. All written consent forms must be stored in a client's case management file for recordkeeping and auditing purposes.

Agencies must make reasonable accommodations for persons with disabilities throughout the data collection process.

Agencies that are recipients of federal assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program.

Definitions and Descriptions of Client Notification and Consent Procedures

Client Notice: A written notice of the functions of the CRN must be posted and can be given to each client so they are aware of the potential use of his/her information and where it is stored. To fulfill this requirement, the agency may either adopt the CRN Notice of Uses and Disclosures or may develop an equivalent Privacy Notice that incorporates all the content of the standard CRN Notice. If the agency has a website, the adopted Notice of Uses and Disclosures or equivalent privacy notice must also be posted on the website

No consent is required for the functions articulated in the notice. However, as part of the notification process, clients must be informed of their right to designate his/her client record as hidden. This client also has a right to view a copy of his/her record upon request.

Client Record: After learning about the CRN, if a client does not wish to have his/her Primary Identifiers accessible to all CRN users, the originating CRN user should indicate on the Intake Screen that the client has requested his/her record remain hidden. A client record will allow the agency to access the client's information for agency purposes. This action will allow CRN Project Manager/System Administrator (as defined in SOP# 03-030: CRN User Access Levels) to view client-identifying information, but will prevent any personal client-identifying information from being accessed by CRN users outside of the originating agency.

Written Client Consent for Interagency Data Sharing: At the initial intake, the Client should be provided an oral explanation and written documentation about the option of sharing his/her General Client Information within the originating agency's Sharing Network. (The specific details of interagency data sharing are described in SOP# 03-080: CRN Interagency Data Sharing.) If a client is interested in sharing his/her General Client Information within the network, he/she must provide written consent. The consent must be specific regarding purpose, the expiration of the sharing, affected data elements, function, and involved parties. The client maintains a right to revoke written authorization at any time, in which case, any currently shared information will become non-shared from that point forward. To fulfill this requirement, the agency may adopt the CRN Client Consent for Network Data Sharing and the Client Revocation of Consent for Network Data Sharing or may develop an internal form that incorporates the content of the standard CRN form.

Written Client Release of Information through the Referral Process: At any point during the case management process, an agency staff member can initiate a referral to another agency. (The specific details of Referral Process are described in SOP# 03-090: CRN Information Sharing Referral Procedures.)

To provide access to client data with a referral, the originating agency must receive a written client release of information that specifically indicates the recipient agency, purpose for sharing, the specific data categories that are being shared, the expiration of the consent, and whether the originating agency has permission to receive information back from the referral agency on the outcome of the referral.

Any client data can potentially be sent through the referral process based on client release. To fulfill this requirement, the agency may adopt the CRN Client Release of Information for

Referrals or may develop an internal form that incorporates the content of the standard CRN form.

Applicability

Each consent method is used for varying purposes and types of agencies. In all cases, the Partner Agency shall uphold Federal and State Confidentiality regulations to protect client records and privacy. If an agency is covered by HIPAA, the HIPAA regulations prevail.

The table below summarizes the client data categories and the related notification/consent and sharing rules that relate to each data category. These minimum procedures should not imply that all providers will perform these functions.

Client Data Categories	**Summary of Notification/Consent & Data Sharing Procedures**
Primary Identifiers: • Name and Aliases* • Birth Date* • Gender • Social Security Number* • Ethnicity • Race • Veteran status • Housing Status • Disabling Condition • Residence Prior to program entry • Zip Code of Last Permanent Address • Program Entry Date • Program Exit Date • Head of Household * These are considered personal identifying data elements.	Non-shared client record: If a client asks to hide his/her primary identifiers, the record will only appear on the Client Search List for the Originating Agency. It will be hidden to all other agencies. Some system-level users will have access to non-shared client records for system administration purposes (as specified in SOP# 03-030). Shared client record: If the client does not ask to hide his/her identifiers, the primary identifiers will be available to all CRN users in the Client Search to locate an existing client as provided in this agency's data sharing agreements. None of the other client information will be viewable, except as described below.
General Client Information: • Family/Relationship Information • Income & Benefits Information • Educational & Vocational History • Housing History • Veteran Information	Non-shared record: If written consent is not provided by the client, this information is only accessible within the Originating Agency and some system-level users for system administration purposes (as specified in SOP# 03-030). Shared record: With written client consent, these data can be shared among a Sharing Network. Any agency can choose to join one Sharing Network. All agencies within a network must execute an Interagency Data Sharing Agreement. Only agencies in that network that are serving that client will be able to view the record. Referrals: Any of these modules can be sent to any other CRN agency for a limited period through the referral process if authorized with a written Client Release of Information.

Client Data Categories	**Summary of Notification/Consent & Data Sharing Procedures**
Protected Information: • Special Needs Screening • Clinical Mental Health Assessment • Clinical Substance Abuse Assessment • HIV/AIDS Information • Domestic Violence Incident Information	Protected Information: This information is only available within the Originating Agency to users that have an authorized access level and to authorize system-level users for system administration purposes. Referrals: Protected information may be shared with other CRN agencies for a limited period through the referral process if authorized by a written Client Release of Information.

Specific Client Notification Procedures for Victims of Domestic Violence

A mainstream agency that is serving a victim of domestic violence must explain the potential safety risks for domestic violence victims and the client's specific options to protect her/his data, such as designating her/his record as 'not-shared' to other agencies. Thus, the client notification process must clearly state the potential safety risks for domestic violence victims and delineate the participation options. As well, all staff must be trained on the protocol for educating domestic violence victims about their individual participation options.

Specific Client Notification Procedures for Unaccompanied Minor Youth

Based on their age and potential inability to understand the implications of sharing information, the CRN cannot be used to share information about unaccompanied minor youth. Thus, even with a written client authorization, users cannot set up interagency data sharing for unaccompanied minor youth. For the purposes of this policy, minor youth are defined as youth under 18.

Privacy Compliance and Grievance Policy

Agencies must establish a regular process of training users on this policy, regularly auditing that the policy is being followed by agency staff (including employees, volunteers, affiliates, contractors and associates), and receiving and reviewing complaints about potential violations of the policy. Agencies may want to appoint a Chief Privacy Officer to be responsible for these tasks.

SOP#: 03-070	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN DATA COLLECTION REQUIREMENTS

Policy: All agencies that provide homeless services are encouraged, and in some cases required, to collect data for all clients served by their programs, as specified by this policy.

Standard: The Partner Agency will develop an interview protocol that facilitates the collection of the required data elements over time, beginning with some elements at intake and obtaining other data over time.

Purpose: To ensure that agencies understand the data collection requirements set by the CRN Steering Committee.

Scope: Partner Agencies

Responsibilities:

Universal Data Elements

The Partner Agency is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements, will be collected and verified from all clients at initial program enrollment or as soon as possible thereafter. Direct Partner Agencies must enter data into the CRN within seven days of collecting the information. Interface Partner Agencies must ensure that the information is captured within seven days in an information system that can generate the information in the prescribed format. Anonymous Data Submittal Partner Agencies must ensure that the information is captured within a timely fashion using a methodology that can generate the information in the prescribed format.

The universal data elements are all included on the Client Tab, Client Supplemental Tab. They include:

- First, Middle, Last Name, and Suffix;
- Social Security Number;
- Date of Birth or estimated Date of Birth (age);
- Ethnicity and Race;
- Gender;
- Veteran Status;
- Disabling Condition (Unless presence of a disability is a condition of program enrollment, disability status must be collected after program admission.);

- Residence Type Prior to Program Entry and Length of Stay;
- Zip code of last Permanent Residence;
- Housing Status
- Program Entry and Exit Dates; and
- Household Affiliation for the purposes of this Program Enrollment;

Agencies are striving to meet a minimum 90% data quality.

Partner agencies must report client-level data for the universal data elements using the required response categories detailed in the Federal Register Part II- Department of Housing and Urban Development - Community Resource Networks, (CRN); Data and Technical Standards Final Notice; This Notice revises the Community Resource Networks (CRN) Data and Technical Standards Final Notice (69 FR 146, August 2016). The Notice adds a new set of Program Description Data Elements (Section 2). In addition, the Notice presents revisions to Data Standards for Universal Data Elements (Section 3) and Program-Specific Data Elements (Section 4). These sections replace Section 2 (Universal Data Elements) and Section 3 (Program-Specific Data Elements) of the 2016 Notice. All other sections of the 2014 notice remain in effect.

Program-specific Data Elements

All Continuum of Care-funded Partner Agencies are also responsible for ensuring that the following assessment data elements, referred to as Program-Specific Data Elements, are collected from all clients that are served by the Continuum funded programs. These program-specific data elements must be entered into the CRN (or alternative approved information system for Interface Partner Agencies) within seven days of collecting the information. The timeframes for data collection are included for each data element.

The Program-specific Data Elements are located throughout the CRN application. Additional information on their location within the CRN will be provided as part of the CRN training materials. They include:

- Income Sources and Amounts (Program Entry and Exit);
- Source of Non-cash benefits (Program Entry and Exit);
- Presence of Physical Disability (Program Entry);
- Presence of Developmental Disability (Program Entry);
- HIV Positive or AIDS Diagnosis (Program Entry);
- Mental Health Status and Chronicity (Program Entry);
- Presence of Substance Addictions and Chronicity (Program Entry);
- History of Domestic Violence and Timeframe (Program Entry);

- Services Received (Throughout Program Enrollment);
- Referrals Provided (Throughout Program Enrollment)
- Destination upon Leaving Program (Program Exit);
- Reasons for Leaving (Program Exit);
- Program Outcomes (Throughout Program Enrollment or at Program Exit); and
- Data quality minimum of 90%

CRN Partner Agencies must provide client-level data for the program-specific data elements using the required response categories detailed in the Federal Register Part II- Department of Housing and Urban Development - Community Resource Networks (CRN); Data and Technical Standards Final Notice; This Notice revises the Community Resource Networks (CRN) Data and Technical Standards Final Notice (69 FR 146, August 2016). The Notice adds a new set of Program Description Data Elements (Section 2). In addition, the Notice presents revisions to Data Standards for Universal Data Elements (Section 3) and Program-Specific Data Elements (Section 4). These sections replace Section 2
(Universal Data Elements) and Section 3 (Program-Specific Data Elements) of the 2016 Notice. All other sections of the 2014 notice remain in effect.

Domestic Violence Anonymous CRN Data Submittal Partner Agency Data Collection Requirements

Data Collection is defined as: a) obtaining client information at the Agency through interview of and/or service provision to the client; and b) the storing of client information at the Agency in paper or electronic format. DV Anonymous CRN Data Submittal (Anonymous Data) Partner Agencies shall collect and store the Universal and Program-specific data elements defined above.

Anonymous Client-level Data are defined as individual client records that contain no personal client identifying information, in whole or in part, or any information that may be used to deconstruct a person's identity. No one beyond the originating agency will have access to any client personal identifying information.

Client personal identifying information is defined as the following data fields:

a) Name(s) or Aliases;
b) Social Security Number;
c) Date of Birth;
d) Mother's Maiden Name;

e) Unique Identifying Characteristics;
f) Address-specific Residence Prior to Program;
g) Unique Person Identifier*; and
h) Any other data fields that may be used to leverage the identity of any individual client.

**A unique client identifier shall be assigned by the Agency to each client. The unique client identifier shall not contain any masked client personal identifying information. The unique client identifier shall not contain, in whole or in part, any client personal identifying information as listed above in fields a) through f). The unique client identifier provides an unduplicated internal count of clients served by the Agency, and provides the CRN Lead Agency the means of conducting longitudinal analysis of services provided to each client.*

With this option, the agency will submit Anonymous Client-level Data to the CRN Lead Agency in an electronic format, per the technical specifications developed by the CRN Lead Agency. The data specifications will be developed by the CRN Lead Agency after discussion with DV Agency leadership and IT staff. The timing and methodology of developing the export functionality to fulfill these data submittal requirements will be subject to agreement between the CRN Lead Agency and the agency. All data should be submitted on a quarterly basis. See SOP# 03-050.

SOP#: 03-080	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:
Title: CRN INTERAGENCY DATA SHARING		

Policy: Data sharing among agencies will be supported upon formalization of data sharing networks by participating agencies.

Standard: For Partner Agencies to engage in data sharing arrangements, a written, formal document must be signed by the Executive Directors of the agencies entering into a network and each client must provide written consent.

Purpose: To formalize the vehicle through which agencies can enter into an agreement allowing such agencies to share client records.

Scope: Partner Agencies wishing to share client-level data.

Background:

Written Agreement: Agencies wishing to share information electronically through the CRN are required to establish a data sharing network in writing by jointly executing an Interagency Data Sharing Agreement, as provided by the CRN Management team.

Role of Executive Director: The Executive Director is responsible for ensuring that users within his/her agency abide by all the policies stated in the Interagency Data Sharing Agreement. Executive Directors wishing to participate in a data sharing network must execute an Interagency Data Sharing Agreement, and identify a lead representative known as the Agency Super User to contact the CRN System Administrator to initiate the process.

Role of CRN System Administrator: Once the Executive Directors of agencies have executed the Interagency Data Sharing Agreement, the Agency Super Users will contact the CRN System Administrator and the System Administrator will establish the Data Sharing in the system.

Client Authorization: Case managers from agencies that have a valid Interagency Data Sharing Agreement may only share client information if the client authorizes that sharing with a valid Client Consent Form, as described in SOP# 03-060: Client Notification Policies and Procedures.

Steps for Establishing an Interagency Data Sharing:

The general steps include:

- Each of the Executive Directors must execute an Interagency Data Sharing Agreement;
- Each participating agency will retain a copy of the agreements and the original will be filed with the CRN System Administrator;
- The CRN System Administrator will establish the data sharing privileges in the system;
- Once data sharing among agencies is established, authorized users will be able to grant permission based on appropriate client consent to share individual client information with all other authorized users in the system; and
- Although data sharing privileges may be established through these actions, authorized users are only able to view client information, beyond the universally shared identifiers, for the clients enrolled in a program within their agency.

Data Sharing protocol will be reinforced by the following technical mechanisms:

- Only authorized users will have CRN access, controlled by user ID and password;
- Each user's access to data will be defined by their user type. Users will only be able to see data categories viewable by their respective user level, regardless of information sharing privileges within an agency;
- CRN System Administrator will need to "authorize" data sharing between agencies before the agencies can begin sharing client information. This authorization will not be

granted unless CRN System Administrator has an executed Interagency Data Sharing Agreement on file;
- Users will only be able to view client data (beyond the universally shared Primary Identifiers) for clients enrolled in a program within their own Agency;
- Protected information (clinical mental health assessment, clinical substance abuse assessment, clinical HIV/AIDS information, and domestic violence incident information) will not be shared. This information will only be viewable by users at the originating agency; and
- Random file checks for appropriate client authorization, audit trails, and other monitoring tools may be used to monitor that this data sharing procedure is followed. Specific monitoring procedures around program enrollment will be implemented to ensure appropriate client information access.

SOP#: 03-090	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN INFORMATION SHARING REFERRAL PROCEDURES

Policy: Agencies will be able to share client information with agencies outside of the Collier County Continuum of Care CRN Network with appropriate written client authorization.

Standard: For Partner Agencies to share client information with agencies outside of the Collier County Continuum of Care CRN Network, a client must provide a written release of information for referral purposes.

Purpose: To formalize the vehicle through which agencies can share data outside of their Collier County Continuum of Care CRN Network Agreements.

Scope: Partner Agencies wishing to share client-level data outside of the Collier County Continuum of Care CRN Network.

Responsibilities:

Any client information stored in the client record of an originating agency may be shared with another Partner Agency based on a written client release of information. Referrals cannot be directed to a specific user at a receiving agency. Users at the receiving agency will only be able to view the client-designated portions of the originating agency's client record based on their user access levels for the timeframe specified in the referral. One or more persons at each agency should be designated to receive incoming referrals daily and direct them to appropriate personnel within the agency.

Since the recipient agency will have an "active window" to the specified portions of the originating agency's file, users within the recipient agency will also be able to see all changes made to the record during the authorized timeframe. The default value for the timeframe for information sharing for referral purposes will be set to fifteen days to limit the privacy and safety risks for clients. Referring agencies will have the opportunity to set an alternative timeframe, if more appropriate. During that timeframe, the recipient agency can print a hardcopy of the client information for archival purposes or can enter client information into its own client record to permanently incorporate the information into its electronic file. At the expiration of that timeframe, the recipient agency will retain a record of the referral but will no longer be able to view the client information. Upon request by the receiving agency and with client consent, the originating agency can extend or re-release the information.

Role of Executive Director: The Executive Director is responsible for establishing and ensuring compliance of all client notification and consent policies stated in the Client Release of Information for Referrals form.

Client Authorization: CRN Users may only share client information if the client authorizes that sharing with a valid Client Release of Information for Referrals form, as described in SOP# 03-060: Client Notification Policies and Procedures.

The general steps include:

- Authorized users will be able to grant permission based on appropriate client consent to share individual client information with another Agency's users; and
- Although data sharing privileges may be established through these actions, authorized users are only able to view client information beyond the universally shared identifiers for clients that enroll in a program within their agency.

Data Sharing protocol will be reinforced by the following technical mechanisms:

- Only authorized users will have CRN access, controlled by user ID and password;
- Each user's access to data will be defined by their user type. Users will only be able to see data categories viewable by their respective user level, regardless of information sharing privileges within an agency or network;
- When a client record is set-up to be accessed by users at another agency, the originating user must obtain client authorization, indicate period of time for data sharing, and specify data categories to be shared;
- Users will only be able to view client data (beyond the universally shared identifiers) for clients enrolled in a program within their agency; and

- Random file checks for appropriate client authorization, audit trails, and other monitoring tools may be used to monitor that this data sharing procedure is followed. Specific monitoring procedures will also be implemented to ensure that clients are being appropriately enrolled in programs.

Section 4 – Security Policies & Procedures

SOP#: 04-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: SYSTEM ACCESS CONTROL POLICIES AND PROCEDURES

Policy: CRN Project Management and participating agency must reasonably secure the system from access by unauthorized users.

Standard: CRN Project Management or its designee and participating agency should employ access prevention and physical access control measures to secure CRN system resources.

Purpose: To protect the security of the CRN system resources.

Scope: CRN Project Management, Agency Executive Director, and Agency Super User

Guidelines:

Central CRN Equipment Access Prevention Mechanism

All computing resources will be protected always by a firewall. User access through the Internet will be controlled using user authentication always.

Physical access to the system data processing areas, equipment, and media must be controlled adequately from the threat of and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment.

The CRN Project Management will determine the physical access controls appropriate for the environment housing the central CRN equipment based on CRN security policies, standards, and guidelines. All those granted access to an area or to data are responsible for their actions. Additionally, if an individual gives access to another person, the authorizing individual is responsible for the other person's activities.

Workstation Access Controls

Access to the CRN will only be allowed from computers specifically identified by the Executive Director and Agency Super User of the participating agency. Laptops will require an additional security form stating that use will not be for unauthorized purposes from unauthorized locations. Access to CRN computer workstations should be controlled through physical security measures

and/or a password. Each Agency Super User will determine the physical access controls appropriate for their organizational setting based on CRN security policies, standards and guidelines. Each workstation should have appropriate and current firewall and virus protection, as specified in SOP# 02-040: CRN Hardware, Connectivity, and Security Requirements.

SOP#: 04-020	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DATA ACCESS CONTROL POLICIES AND PROCEDURES

Policy: CRN Project Management and participating agency must reasonably secure the CRN data from access from unauthorized users.

Standard: CRN Project Management and participating agency should employ access prevention control measures to secure CRN database resources.

Purpose: To protect the security of the CRN database(s).

Scope: CRN Project Management, Agency Executive Director, and Agency Super User

Guidelines:

User Accounts

Agency Super User and the CRN System Administrator must follow the procedures documented in Section 2 for user account set-up, including verification of eligibility, appropriate training, and establishment of appropriate user type. Each user's access to data should be defined by their user type and specific agency data-sharing agreements. Agency Super Users must regularly review End User access privileges and notify the CRN System Administrator to terminate End User IDs and passwords from their systems when End User no longer requires access. It is the responsibility of the End User's supervisor to notify the Agency Super User immediately when an End User leaves the agency or no longer requires access to the CRN system. Unless otherwise terminated or suspended, a user account is valid for one year. The Agency Super User must annually reauthorize an End User to maintain his/her system and database access. Users may be required to attend supplemental training prior to reauthorization.

If a staff person is to go on leave for a period of longer than 30 days, their account should be temporarily suspended within 5 business days of the start of their leave. It is the responsibility of the End User's supervisor to notify the Agency Super User when the End User will be on leave for a period longer than 30 days.

User Passwords

Each user must have a unique identification code (user ID). Each user's identity will be authenticated using a user password. Passwords are the individual's responsibility. Users are prohibited from sharing user IDs or passwords. Sanctions will be imposed on the user and/or agency if user account sharing occurs.

Passwords should be between eight and sixteen characters long and not easily guessed or found in a dictionary. The password format is alphanumeric.

Any passwords written down must be securely stored and inaccessible to other persons. Users should not save passwords on a personal computer for easier log on.

Password Reset

The CRN System Administrator will have the ability to reset a password during non-business hours.

Temporary Suspension of User Access to Database Resources

In the case of system inactivity users must log off from the CRN and workstation if they leave their workstation. CRN Project Management must establish inactivity time-out thresholds to be implemented by the vendor, where technically feasible, for terminals and workstations that access CRN information. Therefore, if a user is logged onto a workstation, and the period of inactivity on the workstation exceeds the designated inactivity period of time the user will be automatically logged off the system.

If a User unsuccessfully attempts to logon six times, the User ID will be "locked out", access permission revoked, and the user will be unable to gain access until his/her password is reset.

Electronic Data Controls

The Partner Agencies must establish internal access policies to data protocols based on the final HUD Data and Technical Standards.

Partner Agencies will have the ability to export a copy of their own data for internal analysis and use. Agencies are responsible for the security of this information.

Hardcopy Data Controls

Printed versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. Media containing CRN client identified data may not be shared with any person or agency other than the owner of the data for any reason not disclosed within the Client Notice. CRN data may be transported by authorized employees using methods deemed appropriate by the participating agency that meet the above standard. Reasonable care should be used, and media should be secured, when left unattended. Magnetic media containing CRN data which is released or disposed of from the participating organization and central server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data. CRN information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

SOP#: 04-030	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: AUDITING POLICIES AND PROCEDURES

Policy: CRN Project Management and Agency Super User will monitor system and database access that could potentially reveal a violation of security protocols.

Standard: CRN Project Management or its designee and Agency Super User will implement a monitoring plan to monitor compliance with data security standards.

Purpose: To protect the security of the CRN system and databases.

Scope: CRN Project Management and Agency Super Users

Guidelines:

Access Monitoring Plan

The CRN application must maintain an audit trail that tracks user log-in attempts for a minimum of six months. The CRN application must also maintain an audit trail that tracks deletions of client records (including the actual assessment entry, date deleted, and username) for a minimum of six months and a record of deleted client records (case number, intake information, date deleted, and username) for a minimum of one year. The CRN application is designed to record transactional data on all other client information for historical and audit purposes. Each entry shall also reflect the user who created the entry and the date and name of the user who made the most recent modification.

The CRN System Administrator must regularly review audit records for evidence of violations or system misuse. The Agency Super User must regularly review the logs for its agency's users to determine unauthorized or inappropriate access to CRN client records.

All users and custodians are obligated to report suspected instances of noncompliance or security violations to an Agency Super User or the CRN System Administrator as soon as possible.

Violations & Sanctions

All potential violations of any security protocols will be investigated by CRN Project Management. Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions include, but are not limited to:

- a formal letter of reprimand;
- suspension of system privileges;
- revocation of system privileges; and

A Partner Agency's access may also be suspended or revoked if serious or repeated violation(s) of the SOPs occur by agency users. All CRN sanctions will be imposed by a team comprised of an CRN User Group Chair, the CRN System Administrator, and the CRN Steering Committee Chair and Chair of the COC Committee. The Board of Directors of the CRN Lead Agency needs to approve the sanctions prior to enforcement.

CRN sanctions can be appealed to a team comprised of the CRN Steering Committee Co-Chair, and the CRN Lead Agency's Board of Directors.

Criminal prosecution sanctions will be recommended by CRN Project Management and the CRN Lead Agency's Board of Directors to the appropriate law enforcement agency.

Section 5 – Internal Operating Policies & Procedures

SOP#: 05-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: SYSTEM AVAILABILITY POLICIES AND PROCEDURES

Policy: The CRN application will be available to users in a manner consistent with the agencies' reasonable usage requirements.

Standard: CRN Project Manager/System Administrator and Software Vendor as hosting and support partner will operate the system full-time and respond immediately in the event of an interruption to service, as defined by the guidelines in this policy.

Purpose: To define system availability.

Scope: CRN Project Manager/System Administrator and Software Vendor

Guidelines:

These guidelines are provided as a reference; however, the official document for system operation is the vendor Hosting and Support Agreement.

Hours of System Operation

The system is designed to be operating and available 24 hours a day 365 days a year. In the unlikely event of an unplanned interruption of service, the vendor is responsible for rapid response and returning the system to online status. For planned interruptions of service the vendor shall schedule these during the least busy times and advise the CRN Project Manager/System Administrator in advance. For regularly scheduled downtimes the vendor shall identify hours, and a set time for planned back-up, security patches, etc. The Project Manager/System Administrator has the authority to determine the definition of 'advance notification' in this situation.

CRN Project Management & System Administrator Availability

The CRN Project Manager/System Administrator will be available during normal business hours (9:00 – 5:00 Monday through Friday). After normal business hours, users should follow the protocols established in SOP# 05-020: Technical Support Policies and Procedures. CRN Project

Manager/System Administrator will be on-call via cell phone in the event of a disaster identified by the CRN Lead Agency.

Planned Interruption to Service

The CRN Project Manager/System Administrator will inform all users via CRN email and/or fax of any planned interruption to service. An explanation of the need for the interruption, expected duration, and benefits or consequences will be provided.

Unplanned Interruption to Service

When an event occurs that makes the system inaccessible and the interruption is expected to exceed two hours,

Hard-Disk Drive Failure

In the case of the primary hard-disk drive failure, our Application Server is housed with an ATA-Raid Controller which is a RAID compliant drive redundancy. The RAID controller will detect the failure and continue operation without interruption of service.

Multiple Hard Drive Failures

In the event of multiple disks failing, a stand-by drive is fully loaded with server requirements and software requirements. Disk is loaded and all backup data collected the day before is loaded to disk. Clients should expect a 2-4-hour lapse of service.

Fire or Natural Disaster
In the event of a fire or natural disaster, offsite data will be loaded into an off-site standby server located offsite. Clients should experience no more than a 3-hour lapse in service with little or no data loss.

SOP#: 05-020	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: TECHNICAL SUPPORT POLICIES AND PROCEDURES

Policy: The CRN Project Manager/System Administrator shall offer standard technical support services to all Partner Agencies and users.

Standard: Users needing technical support on the CRN application should access standard technical support services using the guidelines articulated in this policy.

Purpose: To define technical support services.

Scope: System-wide.

Guidelines:

Technical Support Resolution Procedure – Use of the CRN Application

As unanticipated technical support questions arise, users should implement the following procedure(s) to resolve their questions.

During normal business hours:

- Utilize on-line help resources and/or training materials.
- If question is still unresolved, direct the technical support question to the Agency Super User.
- If question is still unresolved, the Agency Super User can further direct the question to the CRN Project Manager/System Administrator.
- If question is still unresolved, the CRN Project Manager/System Administrator can further direct the question to the vendor technical support staff.

After normal business hours:

- Utilize on-line help resources and/or training materials.
- If issue can wait to be addressed during the following business day, please wait and follow the escalation procedure outlined above,
- If not, then direct the technical support question to the Agency Super User, if available.
- If unavailable, or if the question is still unresolved, contact the CRN Project Manager/System Administrator to determine the appropriate procedure. If the Project Manager/System Administrator determines that the issue needs immediate attention, the request will be forwarded to the vendor technical support. Otherwise, CRN Project Manager/System Administrator may indicate that the user should pursue assistance through normal channels on the following business day.

Technical Support Resolution Procedure – Access to the CRN Application or Database

If a user experiences an unplanned interruption to CRN operation, the user should implement the following procedure to notify the CRN Project Manager/System Administrator and/or understand the status of operations.

During normal business hours:

- Contact your Agency Super User, who should immediately check the status of the agency's ISP.
- If the system outage is unrelated to the agency's internet connectivity, the Agency Super User should contact the CRN Project Manager/System Administrator to immediately report the interruption.
- The Agency Super User should communicate the results of the status update to all agency users who may attempt to use the CRN application during the period of interruption.
- At all times, the CRN Project Manager/System Administrator will provide a central clearinghouse of information about all system interruptions.

After normal business hours:

- Attempt to determine if the interruption is related to the agency's internet connection. (For example, try to access another site on the internet.) If the issue is related to the Agency's internet connectivity, contact the Agency Super User.
- If the system outage is unrelated to the agency's internet connectivity, the user should contact the CRN Project Manager/System Administrator to immediately report the interruption.
- The user should attempt to communicate the results of the status update to other agency users who may attempt to use the CRN application during the period of interruption.
- At all times, the CRN Project Manager/System Administrator will provide a central clearinghouse of information about all system interruptions.

User Training

The CRN Project Manager/System Administrator will provide ongoing CRN software training on a regular basis, as described in SOP# 03-040: CRN Training Requirements. If additional or specific training needs arise, the CRN Project Manager/System Administrator may be able to arrange for special training sessions.

Agency/User Forms

All Agency Super Users will be trained in the appropriate on-line and hardcopy forms. If the Agency Super User has questions on how to complete CRN forms, he/she should contact the CRN Project Manager/System Administrator.

Report Generation

CRN Project Manager/System Administrator shall work with the software vendor in developing and creating the federal mandated reports for the CRN Lead Agency as well as for the Partner agencies, exclusively related to the CRN database.

The CRN User Group will be the primary body to query Partner Agencies on their reporting needs and to prioritize a list of reports to be developed by the CRN System Administrator for all CRN Partner Agencies.

Time permitting, the CRN Project Manager/System Administrator shall aid in developing and creating agency specific reports.

CRN Project Manager/System Administrator shall develop system related reports on usage, access and performance etc. with the software vendor that are derived from the server monitoring tools at the hosting site.

Programming-related Service Requests

If the user encounters programming issues within the CRN application that need to be addressed, the user should identify the error or suggested improvement to the Agency Super User. The Agency Super User should complete an CRN Service Request Form identifying the specific nature of the issue or recommended improvement along with the immediacy of the request.

Service requests will be reviewed by the CRN Project Manager/System Administrator for further action. Requests to fix programming errors or "bugs" will be prioritized and forwarded to the vendor programming team, as appropriate. Suggested application improvements will be compiled and periodically discussed by the CRN Project Manager/System Administrator and the CRN User Group. A prioritized list of improvements will be submitted to the CRN Project Manager/System Administrator for review and submittal to the vendor.

Section 6 – Data Ownership, Usage and Release Policies & Procedures

SOP#: 06-010	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DE-DUPLICATION POLICIES AND PROCEDURES

Policy: The CRN Lead Agency will employ a range of methods to achieve de-duplication to accommodate the unique situations of different provider types.

Standard: The CRN System Administrator and Agency Super Users shall train users on and employ the methods described below to achieve the highest degree of de-duplication.

Purpose: To define the overall de-duplication approach.

Scope: System-wide.

Guidelines:

De-duplication Data Elements

The CRN application will use the following data elements to create unduplicated client records:

- Name (first, middle initial, last, alias);
- DOB (actual or estimated);
- Gender;
- Race and Ethnicity; and
- SSN (full or partial).

The primary way to achieve de-duplication will be a provider-mediated search of the client database prior to creating a new client record. The user will be prompted to enter a minimum number of data elements in the CRN, and a list of similar client records will be displayed.

Based on the results, the user will be asked to select a matching record if the other identifying fields match correctly. If the user is unsure of a match (either because some data elements differ or because of blank information), the user should query the client for more information and/or create a new client record. The user will not be able to view sensitive client information or program-specific information during the de-duplication process. After the client record is selected, the user will only be able to view the previously existing portions of the client record if he/she has explicit authorization to view that client's record, as described in SOP 03-060: CRN Client Notification and Consent Procedures

For providers who do not directly enter data in the CRN and those who do not share information according to the Interagency Data Sharing Agreement, the de-duplication will occur on the back-end using the same client identifiers or a masked ID generated from these identifiers called a Hash Code:

- First letter of the first name;
- Four first letters of the last name;
- Full DOB; and
- Last four digits of SSN.

Data from Interface Partner Agencies can become, but does not have to become, part of the real-time CRN client database. If their data is not merged into the CRN client database, the client records will be integrated into an analytical database.

De-duplication Methods

Agency Type	**Provider-mediated Look-up***	**Backend Central Server Matching based on Identifiable Information**	**Backend Central Server Matching based on Masked Identifier****	**Data Storage Location (Program, Agency, or Server**
Direct Partner Agencies (DPA)	Yes	Yes	Yes	Server
Providers who upload periodic client data	No	Yes	Yes	Agency and Server
DV/MH/Youth/ HIV/AIDS etc. Providers	If DPA	optional	encrypted	Agency/Server

* Hidden client records will not be searchable as part of the provider-mediated look-up. Mainstream providers will be trained on the use of hidden client records for use with victims of domestic violence and/or other clients who deny the right to share their personal information. Hidden records will be unduplicated using one of the backend processes.

** See Definition of a masked identifier below.

Definitions

Provider-mediated look-up: Prior to beginning a new client record, the intake worker or data entry person will search for an existing client record using the de-duplication fields indicated earlier in this SOP.

Hidden Client Data Entry: Primary identifiers are hidden to agency-level users outside of the originating agency, as described in SOP 03-060: CRN Client Notification Policies and Procedures.

Backend Central Server Matching based on Identifiable Information: System-level users will manage a computer-aided process of matching client personal identifying information at the central server level and assigning a common personal identification number to records with similar identifiers for de-duplication purposes. This scenario will be used to produce unduplicated count of hidden client records and will be applied to Collier County Continuum of Care CRN Partner Agency data.
The process will also be used to validate data received from all users, as human error and decisions may introduce error to the provider-mediated look-up process.

Backend Central Server Matching based on Masked Identifier: When primary identifiers are not shared across agencies or shared with the CRN central server for purposes of avoiding duplication, system-level users must complete de-duplication based on a masked identifier. The originating agency must generate a masked identifier based on a CRN-specified algorithm based on elements of the client's personal identifying information. The masked identifiers will be used by CRN system-level users to assign a common personal identification number to records with similar masked identifiers (commonly known as Hash-Code.)

SOP#: 06-020	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DATA QUALITY POLICIES AND PROCEDURES

Policy: All data entered into the CRN and used by the CRN System Administrator or Lead Agency for analytical or reporting purposes must meet the data quality standards.

Standard: The CRN Lead Agency must adopt a data quality plan to ensure that all data meets the data quality standards.

Purpose: To define data quality standards and a data quality management plan.

Scope: System-wide.

Guidelines: **90% minimum data quality expectation**

The CRN Lead Agency shall define a data quality plan that includes specific data quality standards, mechanisms for monitoring data quality, sanctions for non-compliance with standards, and assigned responsibilities.

This policy should be amended to incorporate the data quality plan once the HEARTH ACT guidance is developed.

Current standards are met as outlined by Congress and the Dept of HUD. *"This Notice revises the Community Resource Networks (CRN) Data and Technical Standards Final Notice (69 FR 146, August 2016). The Notice adds a new set of Program Description Data Elements (Section 2). In addition, the Notice presents revisions to CRN Data Standards for Universal Data Elements (Section 3) and Program-Specific Data Elements (Section 4). These sections replace Section 2 (Universal Data Elements) and Section 3 (Program-Specific Data Elements) of the 2014 Notice. All other sections of the 2014 notice remain in effect."*

SOP#: 06-030	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DATA OWNERSHIP POLICIES AND PROCEDURES

Policy: All data usage is governed by the owners of the data.

Standard: Data entered into the CRN or submitted to the CRN Lead Agency for the purposes of the CRN initiative shall be considered owned by the client and agency that collected the information.

Purpose: To define data ownership.

Scope: System-wide.

Guidelines:

The client ultimately retains ownership of any identifiable client-level information that is stored within the CRN. If the client consents to share data, the client, or agency, on behalf of the client, has the right to later revoke permission to share his/her data without affecting his/her right to service.

Identifiable client-level data may only be stored and accessed within the CRN in accordance with the client notification and consent procedures in SOP 03-030: CRN User Access Levels and SOP 03-060: Client Notification Policies and Procedures.

In cases where agencies and clients agree to share identifiable client-level data, this information may only be shared in accordance with SOP 03-060: CRN Client Notification Policies and Procedures, SOP 03-080: CRN Interagency Data Sharing, and SOP 03-090: CRN Information Sharing Referral Procedures

If the relationship between the CRN and a Direct Partner Agency is terminated, the agency will retain ownership of the identifiable client-level data that has been submitted to the CRN. The CRN staff shall make reasonable accommodations to assist a Direct Partner Agency to export their data in a format that is usable in an alternative database. In this circumstance, any agency-entered client-level data must be de-identified in order to remain in the CRN database. This de-identified information shall remain available to the CRN Lead Agency for analytical purposes. For the purposes of de-identification, the personal identification number shall not be considered an identifying data element if it is not stored with any other personal identifiers.

SOP#: 06-040	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DATA CLASSIFICATION POLICIES AND PROCEDURES

Policy: All data entered into or generated by CRN shall be managed according to their classification system.

Standard: All data must be classified public, internal, or confidential. All data must be handled per its classification. Failure to handle data properly is a violation of this policy.

Purpose: To define data classifications.

Scope: System-wide.

Guidelines:

Definitions

Public Data: Information published per Data Release policies. See SOP# 06-060.

Internal Data: Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, or data without context.

Confidential Data: Information that identifies clients contained within the database. Examples include social security number, name, address, or any other information that can be leveraged to identify a client. Specific identifiable data elements are described in the CRN Data Collection Requirements SOP# 03-070.

Procedures for Transmission and Storage of Data

Public Data does not require security controls.

Internal Data is accessible only to internal employees. No auditing is required. No special requirements are necessary for the destruction of this data. This data must be stored securely and can be transmitted via internal or first class mail.

Confidential Data requires encryption at all times. It must be magnetically overwritten and the destruction must be verified by database administrator. Hardcopies of confidential data must be produced only for specific, short-term analysis and appropriately destroyed following completion of the task. This data can only be delivered by hand to data owner.

SOP#: 06-050	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: CRN DATA USES AND DISCLOSURES POLICIES AND PROCEDURES

Policy: All CRN stakeholders will follow the data disclosure policies and procedures to guide the use and disclosure of client information stored in or generated by the CRN.

Standard: This policy establishes the CRN Lead Agency-approved uses and disclosures for CRN client data.

Purpose: To define minimum standards for data disclosure.

Scope: System-wide.

Guidelines:

Each CRN Partner Agency must comply with the following Uses and Disclosures, as outlined in the standard CRN Notice of Uses and Disclosures. A Partner Agency has the right to establish additional uses and disclosures if they do not conflict with the CRN Lead Agency-approved uses and disclosures.

Privacy Notice Requirement

Each agency must either adopt the standard CRN Notice of Uses and Disclosures or develop an alternative Agency Privacy Notice that incorporates the content of the standard CRN notice. Every agency must post the notice and/or provide a copy of the notice to each client, in accordance with SOP 03-060: CRN Client Notification and Consent Procedures. If an agency maintains a public web page, the agency must post the current version of its privacy notice on the web page.

An agency's Privacy Notice must:

- Specify all potential uses and disclosures of client personal information;
- Specify the purpose for collecting the information;
- Specify the period of time for which the data will be retained at the agency and the method for disposing of it or removing identifiers from personal information that is not in current use seven years from when it was created or last modified;
- State the process and applicability of amendments, and commit to documenting all privacy notice amendments;

- Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process
- Allow the individual the right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand; and
- Specify a procedure for accepting and considering questions or complaints about the privacy and security policies and practices.

CRN Lead Agency-approved Uses and Disclosures

CRN client data may be used or disclosed for (1) case management, (2) administrative, (3) billing, and (4) analytical purposes. Uses involve sharing parts of client information with persons within an agency. Disclosures involve sharing parts of client information with persons or organizations outside of an agency.

- **Case Management Uses and Disclosures:** Agencies may use or disclose client information for case management purposes associated with providing or coordinating services. Unless a client requests that his/her record remain hidden, personal identifiers will be disclosed to other CRN agencies so other agencies can easily locate the client's record if he/she goes to them for services. Beyond personal identifiers, each agency can only share client information with other agencies with written client consent.
- **Administrative Uses and Disclosures:** Agencies may use client information internally to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions. Client information will be stored on a central case management database; as such, client information will be disclosed for system administration purposes to CRN Project Manager/System Administrator and Data Systems International employees or other contractors who administer the central database.
- **Billing Uses and Disclosures** include functions related to payment or reimbursement for services. An example might include generating aggregate reports for the people and organizations that fund an agency. A client's personal information may be disclosed for billing purposes if required by the service providers.
- **Analytical Uses and Disclosures:** Agencies may use client information for internal analysis. An example would be analyzing client outcomes to evaluate program effectiveness. Agencies will disclose client personal identifiers to the central system administrators for uses related to creating an unduplicated database on clients served within the system, ultimately resulting in the creation of de-identified personal information. Agencies may also disclose portions of a client's information without the personal identifiers for analytical purposes related to analyzing client data, including, but not limited to, understanding trends in homelessness and needs of persons who are

homeless, and assessing the implementation of the Continuum's 10-Year Plan to End Homelessness.

In accordance with the Housing and Urban Development Data and Technical Standards Final Notice, a client's information may also be used or disclosed for such purposes: 1) as required by law; 2) as necessary to avert a serious threat to health or safety; 3) to report victims of abuse, neglect or domestic violence; 4) academic research purposes; and 5) law enforcement purposes only in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial office or a grand jury subpoena.

SOP#: 06-050	Title: CRN DATA USES AND DISCLOSURES POLICIES AND PROCEDURES
	Page 3

A client record will be stored on the Bowman Service Point CRN system with personal identifiers.

Clients have right to request the CRN Privacy & Security Policies from the CRN Lead Agency or via a User Agency.

SOP#: 06-060	Revision:	Prepared by: CRN
Approval Date: Pending	Revision Date:	Revised by:

Title: DATA RELEASE POLICIES AND PROCEDURES

Policy: All CRN stakeholders will follow the data release policies and procedures to guide the release of client information stored in or generated by the CRN.

Standard: Data must be categorized as confidential or internal unless it meets the data release policy.

Purpose: To define standards and circumstances for data release.

Scope: System-wide.

Guidelines:

Client-identified data

No identifiable client data will be released to any person, agency, or organization that is not the owner of said data for any purpose other than those specified in SOP 06-050: CRN Data Uses and Disclosure Policies and Procedures without written permission from the owner.

Data Release Criteria

CRN client data will only be released in aggregate or anonymous client-level data formats for purposes beyond those specified in SOP 06-050: CRN Data Uses and Disclosure Policies and Procedures, per the criteria specified below.

Aggregate Data Release Criteria:

- All data must be anonymous, by removal of all identifiers and all information that could be used to infer an individual or household's identity;
- Aggregate Data must represent sixty percent (60%) of the clients in that universe (program, agency, subpopulation, geographic area, etc.), unless otherwise required for the Congressional AHAR;
- Only Partner Agencies can authorize release of aggregate, program-specific information beyond the standard reports compiled by the Continuum of Care for funding purposes. There will be full access to aggregate data for all participating agencies;
- Parameters of the aggregate data (e.g. where the data originates, what it includes and what it does not include) will be presented to those requesting aggregate data; and
- Released aggregate data will be made available in the form of an aggregate report or as a raw dataset

Anonymous Client-level Data Release Criteria:

- All data must be anonymous by removal of all identifiers and all information that could be used to infer an individual or household's identity;
- Program specific information will not be released without the written consent of the agency's Executive Director; and
- Parameters of the data (e.g. where the data originates, what it includes and what it does not include) will be presented to those requesting aggregate data.

Data Release Process

Beyond individual agency reports or Continuum of Care reports on its funded programs, the CRN Lead Agency Executive Director must approve data for public classification and release.