

---

# MA-503 Cape Cod and Islands CONTINUUM OF CARE

---

Homeless Management  
Information System  
HMIS POLICIES AND  
PROCEDURES MANUAL

---

Version 5.0

UPDATE May 2023

---

## CONTENTS

---

<b>SECTION 1: HMIS OVERVIEW .....</b>	<b>6</b>
Definition of Homeless Management Information System (HMIS) .....	6
HUD HMIS Requirement .....	6
Cape Cod and Islands COC: HMIS Lead and System.....	6
Covered Homeless Organizations (CHOs) .....	7
Governance .....	7
Definitions of Key Terms .....	7
Policy Review and Amendment .....	9
Privacy, Security and Data Quality Plans.....	9
<b>SECTION 2: PARTICIPATION IN HMIS .....</b>	<b>10</b>
Contribution of Data .....	10
Participation Agreement.....	10
CHO HMIS Agency Administrator.....	10
Technological Requirements for Participation .....	11
Agency Profiles in HMIS .....	11
Authorization of HMIS Users - Access to HMIS .....	11
End User Agreement Document Retention .....	11
Training .....	11
Removing Authorized Personnel.....	12
<b>SECTION 3: DATA COLLECTION .....</b>	<b>13</b>
Collection of Data on Participants and Non-Participants.....	13
Required Data Elements.....	13
Project Descriptor Data Elements.....	13
Universal Data Elements .....	13
Program Specific Data Elements .....	13
Federal Partner Specific Data Elements .....	14

Coordinated Entry Data Elements.....	14
Data Collection Standards and Assessments .....	14
Intake and Assessment Forms.....	14
Project Entry Assessment.....	15
Project Update Assessment .....	16
Project Annual Assessment.....	16
Project Exit Assessment .....	16
Domestic Violence and Comparable Databases .....	16
Client Record Retention .....	16
<b>SECTION 4: DATA QUALITY PLAN.....</b>	<b>17</b>
Data Quality.....	17
Reducing Duplicates .....	17
Improving Data Quality .....	17
Data Quality Benchmarks and Controls .....	17
Roles and Responsibilities .....	17
Cape Cod and Islands CoC .....	17
HMIS Committee .....	17
HMIS Lead - Barnstable County.....	17
Covered Homeless Organizations .....	18
Remedial Actions.....	18
<b>SECTION 5: COMPLIANCE AND TECHNICAL ASSISTANCE .....</b>	<b>20</b>
<b>SECTION 6: SECURITY PLAN .....</b>	<b>21</b>
Security Officers .....	21
Identification of CHO HMIS Security Officer .....	21
Annual Security Certification .....	22
Security awareness training and follow-up.....	22
Reporting security incidents .....	22

Security Incidents .....	22
Reporting Threshold.....	22
Reporting Process .....	22
Audit Controls .....	22
System Security .....	23
User Authentication .....	23
Virus Protection.....	23
Firewalls .....	23
Physical Access to Systems with Access to HMIS Data .....	23
Hard Copy Security.....	23
Electronic Communication .....	25
Database Integrity .....	24
Disaster Recovery.....	24
Contracts and other arrangements.....	24
<b>SECTION 7: PRIVACY PLAN and NOTICE SIGN .....</b>	<b>26</b>
Data Collection Notice.....	26
Privacy Notice.....	26
Accountability.....	26
Access and Correction .....	26
Purpose and Use Limitations.....	27
Confidentiality .....	27
Protections for Victims of Domestic Violence, Dating Violence, Sexual Assault, and Stalking .....	28
Other Requirements.....	28
Certain Protected Health Information .....	28
<b>APPENDICES.....</b>	<b>29</b>
Appendix 1: HMIS Participation Agreement .....	29

Appendix 2: Designation of Agency Administrator Form.....	36
Appendix 3: End User Request Form .....	37
Appendix 4: Data Collection Templates – Intake and Entry Assessment.....	39
Appendix 5: Data Collection Templates – Project Annual / Update Assessment .....	42
Appendix 6: Data Collection Templates – Project Exit Assessment.....	44
Appendix 7: Data Quality Benchmarks.....	46
Appendix 8: Identification of Security Officer .....	47
Appendix 9: Security Compliance Certification.....	48
Appendix 10: WellSky Data Recovery Plan .....	51
Appendix 11: Data Collection Notice .....	71
Appendix 12: Privacy Notice – English .....	72
Appendix 13: Privacy Notice – Spanish .....	74
Appendix 14: Authorization for the Release of Protected Information.....	76

## SECTION 1: HMIS OVERVIEW

---

### Definition of Homeless Management Information System (HMIS)

A Homeless Management Information System (HMIS) is a locally administered electronic data collection tool used to record and store client-level information about the numbers, characteristics, and needs of homeless and at-risk persons who use housing and supportive services or homelessness prevention services.

HMIS is essential to coordinate client services and guide community planning and public policy. Through HMIS, homeless households benefit from improved coordination within and among agencies, informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered through HMIS is critical to the preparation of a periodic accounting of homelessness in the Cape Cod and Islands Continuum of Care (CoC), including required HUD reporting.

### HUD HMIS Requirement

Since 2004, HUD has required recipients of Continuum of Care (CoC) Program funds to collect electronic data on their homeless clients in HMIS. HUD published the HMIS Data and Technical Standards in the Federal Register in 2004, specifying the data elements and standards that guide HMIS data collection across the country, standardizing data collection nationally, and describing how data is to be collected and safeguarded.

### Cape Cod and Islands COC: HMIS Lead and System

The Cape & Islands Regional Network on Homelessness Policy Board has designated Barnstable County as the CoC's HMIS Lead entity. Barnstable County serves as HMIS System Administrator/Security Officer to ensure the quality of data entered in the database and to support general usage by all programs using the system. Barnstable County is also responsible for monitoring compliance with HUD Data Standards and CoC policies, for developing necessary reports, and for overseeing privacy and security policies.

The CoC is responsible for selecting the HMIS software product, which serves as a web-based direct data entry portal. The CoC has chosen WellSky's *Servicepoint/Community Services* as its HMIS software. Each agency that participates in HMIS has its own HMIS site, and each agency controls its own data sharing. Non-CoC funded participating agencies that do not use the CoC's HMIS software may participate in HMIS using other products, providing that the software:

- Can collect HUD Universal and Common Data Elements, and
- Can generate HUD reports in Comma Separated Values (csv) files for upload into the CoC's HMIS.

## Covered Homeless Organizations (CHOs)

All Cape and Islands CoC recipients of grants from programs authorized by the HEARTH ACT Program Rule Title IV of the McKinney-Vento Act are required to contribute data to the CoC's HMIS, except for victim service providers.<sup>1</sup> In addition, all other non-CoC agencies providing shelter, housing, and services to homeless and at-risk populations are strongly encouraged to use the Cape and Islands CoC HMIS database.

An agency that participates in HMIS is referred to as a Covered Homeless Organization (CHO). CHOs are responsible for their client level data, are responsible for the integrity and security of their agency's client level data and are liable for any misuse of the system by agency staff. CHOs must ensure that their agency users comply with the policies and procedures outlined in this manual.

## Governance

The Cape Cod and Islands CoC adopted an HMIS Governance Charter in September 2013 (updated June 2020), which defines the roles and responsibilities of the CoC, the HMIS Lead, CHOs, and the HMIS Committee. These HMIS Policies and Procedures incorporate the terms of the HMIS Governance Charter.

## Definitions of Key Terms

The section below defines key terms used throughout this document and HUD guidance regarding HMIS.

- **Client Level Data** – (see **Personally Identifiable Information**, below)
- **Comparable Database** - A database that is not the CoC's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information entered into a comparable database must not be entered directly into or provided to an HMIS.
- **Continuum of Care (CoC)** - The group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities,

---

<sup>1</sup> Victim services providers are prohibited from entering client data into HMIS and must instead enter required data into a HUD compliant comparable database.

affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless participants organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.

- **Data Recipient** - A person who obtains Personally Identifiable Information (PII) from an HMIS Lead or from a CHO for research or other purposes not directly related to the operation of the HMIS, the CoC, the HMIS Lead, or the CHO.
- **Homeless Management Information System (HMIS)** - The information system designated by Continuums of Care to comply with the requirements of 24 CFR part 580 and used to record, analyze, and transmit client and activity data regarding the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.
- **HMIS Lead** - The entity designated by the Continuum of Care in accordance with 24 CFR part 580 to operate the CoC's HMIS on its behalf. The HMIS Lead for the Cape Cod and Islands CoC is Barnstable County Department of Human Services.
- **HMIS System Administrator**– The person responsible for all facets of the day-to-day operation and maintenance of the HMIS. The HMIS System Administrator is employed by the HMIS Lead.

**HMIS Vendor** - A contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, and provider of other information technology or support.

- **Identifiable Information (PII)** - Client level, personal information that can be used to determine a program participant's identity, either when used alone or when combined with other information, such as full name, date of birth, Social Security Number, etc. Some Client Level data is not considered PII because, when used on its own, it cannot identify a specific client, such as age, gender, or race. For the sake of convenience, in this HMIS Policies and Procedures manual, the term **Client Level Data** may be used interchangeably with **PII**.
- **Unduplicated Accounting of Homelessness** - An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless participants), utilization of homelessness programs over time, and the effectiveness of homelessness programs.



- **User** - An individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.
- **Victim Service Provider** - A private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, including rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

## Policy Review and Amendment

On an annual basis, the HMIS Lead and the HMIS Committee will review the HMIS Policy and Procedures Manual to ensure compliance with HUD regulations/technological changes.

If policy changes are necessary, the HMIS Lead will submit recommendations for revisions to the HMIS Committee, who will review the suggested policy updates. The HMIS Committee will forward recommendations to the Cape & Islands Regional Network on Homelessness Executive Committee, who will in turn present the recommended policy revisions to the Cape & Islands Regional Network on Homelessness Policy Board (Policy Board). The policy revisions will be reviewed and voted on by the Policy Board. The HMIS Lead will modify practices, documentation, and training material to be consistent with the revised policies within six (6) months of approval.

## Privacy, Security and Data Quality Plans

The HMIS Lead, in consultation with CHOs and the CoC, is responsible for the creation and annual updating of Privacy, Security, and Data Quality Plans which conform to HUD requirements. These Plans are incorporated into these policies and procedures and must be complied with by the HMIS Lead and all CHOs.

## SECTION 2: PARTICIPATION IN HMIS

---

### Contribution of Data

Data are contributed to HMIS in one of two ways:

- Entered directly into the Cape Cod and Islands CoC HMIS. Agencies that contribute directly are provided web-based log-in information with which to access the system.
- Entered into a client management information system operated by a CHO that allows for the collection of the minimum required data elements and that can generate Comma Separated Value (csv) files formatted to meet HUD standards. Data will be transferred into the HMIS using File Transfer Protocol (FTP) administered by the HMIS software vendor.
- Entered into the Massachusetts (MA) Rehousing Data Collective (RDC) data warehouse. The CoC will have access to the data through the CoC's RDC account. CHOs must create their own accounts with the RDC and execute their own Data Sharing Agreements with the MA Department of Housing and Community Development (DHCD), which administers the RDC.

### Participation Agreement

All CHOs that participate in the Cape Cod and Islands CoC's Servicepoint/HMIS platform must sign and agree to abide by the terms of the MA-503 Cape Cod and Islands HMIS Participation Agreement ([Appendix 1](#)).

### CHO HMIS Agency Administrator

Each CHO must designate a single agency representative to act as the CHO's HMIS Agency Administrator ([Appendix 2](#)). CHO HMIS Agency Administrators are responsible for the following:

- Communicate personnel/security changes for HMIS users to the Cape Cod and Islands CoC HMIS System Administrator
- Act as the first tier of support for agency HMIS users
- Oversee training for new Agency end users
- Act as the liaison or contact between the agency and Cape Cod and Islands CoC HMIS Administrator
- Ensure that the agency adheres to client privacy, confidentiality, and security policies
- Maintain compliance with technical requirements for participation
- Store and enforce end user agreements
- Deactivate users who are no longer authorized to have access to HMIS

- Ensure that the Privacy Notice is posted at all intake points and on the Agency's website and that the Data Collection Notice is offered to all individuals who share PII for entry into HMIS
- Enforce data collection, entry, and quality standards
- Attend trainings and technical assistance as offered

## Technological Requirements for Participation

All computers accessing the Cape Cod and Islands CoC HMIS on behalf of the agency must meet the minimum system requirements as outlined in the HMIS Security Plan, which is incorporated into these policies and procedures.

## Agency Profiles in HMIS

Each agency must be set up in HMIS, with profiles that define the programs and services the agency offers, prior to HMIS use and data entry. Agencies should contact the Cape Cod and Islands CoC HMIS Administrator for agency set up. Agency Profiles will be reviewed and updated on an annual basis.

## Authorization of HMIS Users - Access to HMIS

To add a new agency HMIS User, a CHO must submit a completed copy of the HMIS End User Agreement ([Appendix 3](#)) to the HMIS Lead. By submitting the End User Agreement, the CHO HMIS Agency Administrator verifies that the new user has completed the necessary privacy and security training, as well as End User training (training videos may be found on HMIS webpage: <https://www.capecod.gov/departments/human-services/initiatives/housing-homelessness/home-management-information-systems-hmis/>). The Agency Administrator provides each new HMIS user with a unique username and temporary password. The HMIS user must change the password the first time he/she logs into the system.

The HMIS System Administrator will confirm with each Agency Administrator the list of approved agency users on a quarterly basis.

## End User Agreements Document Retention

HMIS End User Agreements must be signed and kept by CHOs for all agency personnel or volunteers that will collect or use HMIS data on behalf of the agency. Agencies must store original HMIS User Agreements for five (5) years after revoking an individual's authorization or in terminating an individual's employment.

## Training

The CoC hosts a self-service library of HMIS technical videos on its webpage:

<https://www.capecod.gov/departments/human-services/initiatives/housing-homelessness/home-management-information-systems-hmis/>. Videos address a variety of topics (such as Data Privacy

and Security, New End User Training, Agency Administrator Training, Coordinated Entry Training, Case Manager Training, Youth and Young Adult (YYA) Grant Training), and new videos are added as they become available. New users are expected to complete the Data Privacy and Security Training video and the New End User Training video prior to being issued a system user license. The HMIS System Administrator also provides both scheduled and ad hoc written, in-person, and virtual trainings that can be customized to meet the needs of the HMIS users.

Trainings in system use for CHO HMIS Agency Administrators are formatted as a “train-the-trainer” model, in which Agency Administrators will oversee the training of their CHO’s HMIS users in system navigation and data input.

## Removing Authorized Personnel

Agency Administrators must immediately deactivate user accounts for individuals who are no longer authorized to access HMIS on the agency’s behalf and notify the HMIS System Administrator in writing within 24 hours. The HMIS System Administrator must update the list of authorized users in HMIS.

## SECTION 3: DATA COLLECTION

---

### Collection of Data on Participants and Non-Participants

Agencies should collect data from households and individuals who are homeless or at risk of becoming homeless and are accessing services from their agency. Agencies may also choose to collect data for HMIS on individuals or households that make contact with the agency but are not able to receive services from the agency. Information must be collected separately for each household member, and all household members' data must be entered into the database.

#### Required Data Elements

The FY2022 HUD HMIS Data Standards outline three categories of required data elements: Project Descriptor Data Elements, Universal Data Elements (Universal Identifier Elements and Universal Project Stay Elements), and Program Specific Data Elements.

#### Project Descriptor Data Elements

Project descriptor data elements (PDDE) are intended to identify the organization, specific project, and project details to which an individual client record in an HMIS is associated. They are created at initial project setup within the HMIS and should be reviewed at least once annually and as often as needed to ensure that reporting is accurate. The HMIS Lead Agency must ensure that the HMIS includes project descriptor information for all projects participating in HMIS. Project descriptor data elements required for project setup in HMIS include Organization Information, Project Information, Continuum of Care Information, Funding Sources, and Bed and Unit Inventory Information.

#### Universal Data Elements

Universal Data Elements (UDE) are to be collected for all households and individuals by all projects participating in HMIS, regardless of funding source, as part of the Continuum of Care's HMIS implementation. A complete list of current HUD UDEs may be found at <https://www.hudexchange.info/programs/hmis/hmis-data-standards/>.

#### Program Specific Data Elements

To meet the statutory and regulatory requirements of federally funded programs using HMIS, additional elements are required for different funding sources. Program Specific Data Elements (PSDE) are required by some HMIS federal partner programs and are necessary to complete Annual Performance Reports (APRs) required by programs that receive funding under the McKinney-Vento Homeless Assistance Act. A complete list of current HUD PSDEs may be found at <https://www.hudexchange.info/programs/hmis/hmis-data-standards/>.

### Federal Partner Program Elements

Federal Partner Program Elements (FPPEs) are additional data elements that apply specifically to one of the individual Federal Partner Programs (Continuum of Care [CoC], Housing Opportunities for Persons with Aids [HOPWA], Projects for Assistance in Transition from Homelessness [PATH], Runaway and Homeless Youth [RHY], Rural Housing Stability Assistance Program [RHSAP], and Veterans Administration [VA]). These data elements must be collected by federally funded agencies as a requirement for them to be considered CHOs. A complete list of current FPPEs may be found at <https://www.hudexchange.info/programs/hmis/hmis-data-standards/>.

### Coordinated Entry Data Elements

Coordinated Entry (CE) Data Elements are intended to standardize data collection on core components of CE -- access, assessment, referral, and prioritization.

- CE Assessment – the CoC may define its own assessment questions and responses
- CE Event – designed to capture access and referral events, as well as the results of those events
- Current Living Situation – records where a person is staying at a point in time, can be updated at each point of contact to track how the client moves

## HMIS Data Collection Standards and Assessments

### Intake and Assessments

Each new client file in HMIS requires certain basic information to be collected, including name, date of birth, social security number, gender, race, ethnicity, primary language, and veteran status (all adults). These Universal Data Elements are collected as part of the intake process.

Project Specific Data Elements are collected as part of the Project Entry Assessment. It is important to note that the assessment date must reflect actual date on which the participant was assessed, not the date of data entry. In addition, project start date and entry assessment date must match for each participant entered in the program. A Data Collection and Project Entry Assessment Template may be found in [Appendix 4](#).

There are three other HMIS assessments used by the CoC for data collection: Annual Assessment and Update Assessment (both [Appendix 5](#)) and Exit Assessment ([Appendix 6](#)).

All programs must use the Project Entry and Project Exit Assessments. Agencies receiving funds from federal homeless assistance grants are additionally required to use the Project Annual Assessment and Project Update Assessment forms. The CoC urges all CHOs, regardless of funding source, to gather and submit data through all four Assessments to provide a more complete picture of homelessness in the Cape and Islands Region. The additional data points

can prove extremely helpful for the agency when reporting on client outcome measurement/progress, internal accounting for service delivered, and external reporting to funders.

### Project Entry Assessment

The Project Entry Assessment is used ensure that new clients are entered into HMIS with the required data elements and assigned to a program with the correct entry date. Program entry and exit dates are required to determine a client's length of stay in the program, the client's patterns of homelessness, and daily capacity rates of the program. Entry and exit dates differ for program types, however the Cape and Islands CoC expects the following standards for each program type.

- **Street Outreach** programs are required to enter clients into the program on the date of first contact with the client.
- **Emergency Shelters for Individuals** are required to enter clients into the program on the first night of stay in the shelter and assigned a bed using the HMIS bed register on a daily basis when residing in the shelter. Individual emergency shelter clients who have been entered into the program on their first night of stay and have not returned after 30 days must be exited from the program using the last night in the bed as the program end date and exit assessment date.
- **Emergency Shelters for Families** are required to enter clients into the program on the first night of stay in the shelter and assigned a bed using the HMIS Emergency Assistance (EA) bed register. Family members departing shelter must be exited out of the program when they leave the program.
- **Transitional Housing Programs** are required to assign entry dates to clients when they move into the program and exit dates when they leave the program.
- **Permanent Supportive Housing Programs and Rapid Rehousing Programs** are required to assign Project Start dates for all clients and Move In dates for households that become housed and to exit clients when they leave the program, using the required Program Specific Data Elements for both entry and exit.
- **Other Service Projects** (including but not limited to: Supportive Services Only, Day Shelter, Homelessness Prevention, Coordinated Entry) should enter clients with an entry date when the client first began working with the project and received the first provision of service and exit the client from the program when the client's case has been closed.

Failure to assign entry and exit dates to a client will result in non-compliance with the Cape Cod and Islands CoC HMIS Data Quality Standards and may negatively impact the CoC's application score in the annual Notice of Funding Opportunity (NOFO) Competition.

### Project Update Assessment

Update Assessments are used when there are changes in a participant's situation, including but not limited to, increase in income, diagnosis of disability, reduced or increased household size, etc., between the Entry Assessment and Exit Assessment. There is no limit to the number of update assessments that can be entered.

### Project Annual Assessment

All federally funded Permanent Housing and Rapid Rehousing programs are required to complete Annual Assessments for all participants each year (within 30 days before or after the head of household's project start date anniversary) until the individual or family members exit the program. The expectation is that Annual Assessments will be conducted for all program participants that have been enrolled in projects for 12 months or more. Ongoing assessments and updating of participant information enables the program and the CoC to assess progress toward housing stability, increased income, and increased access to mainstream benefits.

### Project Exit Assessment

The Exit Assessment provides the date the client left the program, information on the participant's status at exit, and the participant's housing destination. The CoC expects all programs to complete Exit Assessments for all exiting participants and to ensure that Exit Assessment dates match the actual dates that clients leave the programs. Intermittent participants must be entered and exited from programs for each intermittent stay.

### Domestic Violence and Comparable Databases

Domestic Violence programs are prohibited from participating in HMIS, per the Violence Against Women Act (VAWA) section 3 "Universal Grant Conditions: Nondisclosure of Confidential or Private Information" and section 605 "Amendment to the McKinney-Vento Homeless Assistance Act". Victim Services Providers (VSP) that receive funding from any HMIS mandated source are required to collect all the same HUD data elements and assessment information in a separate, comparable database and to submit aggregated, de-identified data to the HMIS Lead for reporting purposes.

## HMIS Client Record Retention

Client records will be retained in HMIS for a minimum period of seven (7) years from the date of project enrollment.



## SECTION 4: DATA QUALITY PLAN

---

### Data Quality

The value of HMIS depends on the quality of the data entered into the system. All programs must strive to provide the most accurate and consistent data as is possible.

#### Reducing Duplicates

Users should ensure that duplicate records are not created within the system by conducting a thorough client search at intake. If duplicates are created, the CHO must work with the HMIS System Administrator to merge the duplicate records.

#### Improving Data Quality

All CHOs must comply with standards set forth in this Data Quality Plan, which is incorporated into these HMIS Policies and Procedures.

### Data Quality Benchmarks and Controls

As part of its data quality plan, the CoC follows the Data Quality Benchmarks found in [Appendix 7](#). The chart identifies the standards that the CoC will monitor, as well as the monitoring procedures for each standard. The Coverage standard applies to the CoC as a whole, while all other standards apply to CHOs and programs.

### Roles and Responsibilities

#### Cape Cod and Islands CoC

The Cape Cod and Islands CoC is responsible for oversight of data quality and will review high-level data quality reports quarterly. The Policy Board will act upon recommendations made by the HMIS Committee and the HMIS Lead.

#### HMIS Committee

The HMIS Committee is responsible for ongoing oversight of progress toward meeting all CoC goals as stated in the Data Quality Plan. The Committee will review data quality reports as requested by the HMIS System Administrator, review the HMIS Policies and Procedures manual on an annual basis, review Data Quality Benchmarks on an annual basis, review Security and Privacy policies on an annual basis, oversee the annual HMIS Site Visit, and convene as necessary to address system wide data quality issues.

#### HMIS Lead – Barnstable County

The HMIS Lead is responsible for monitoring CHOs to ensure that data quality standards are met to the greatest possible extent and that data quality issues are quickly identified and resolved. The HMIS Lead is also responsible for training Agency Administrators and for providing technical assistance as necessary to complete required reports on a timely basis.

Regularity of reporting provides participating agencies with the opportunity to review data and update any missing elements before the HMIS System Administrator assesses progress.

The HMIS lead will run monthly system-wide Data Quality Reports and provide to the Regional Network on Homelessness Policy Board Executive Committee (EC) a Data Quality report at each monthly meeting. These reports will be made available for CoC program performance monitoring. CHO's will be notified of data quality problems by the HMIS Lead with recommendations for resolution:

- **Missing / Incomplete Data Elements:** CHO has failed to enter complete universal and/or program specific data elements.
- **Missing / Incomplete Assessments:** CHO has failed to record required assessments (entry, update, annual exit), or detailed information is missing from project assessments.
- **Incomplete Responses:** CHO has recorded incomplete responses, which are considered as "No Response" by HUD reporting standards.

The HMIS System Administrator will train one person from each CHO to run the monthly Data Quality Reports for all the agency's projects. These reports should be used to identify areas of inaccurate, incomplete, or missing data.

As part of the **CoC Annual Grantee Site Visit**, the HMIS Administrator will monitor the CoC-funded projects to review data quality reports, bed utilization reports, and compliance with the Data Quality Plan; will report to the HMIS Committee on the quality and usability of data submitted by CoC-funded agencies; and will make recommendations to the HMIS Committee for improvements in data quality.

#### Covered Homeless Organizations

CHO's are responsible for overseeing the training of and monitoring HMIS users to ensure understanding of and compliance with data quality standards.

Each CHO is responsible for addressing any issues identified through the data quality monitoring. Where data errors are identified, the CHO must correct the errors within five (5) days of discovery of the errors or contact the HMIS lead if they need more time or additional assistance. Where overall systemic data quality issues are identified, the CHO must participate with the HMIS Lead in creation of a corrective action plan.

#### Remedial Actions

The CoC's goal of data quality monitoring is to obtain and maintain high-quality data. To meet this goal, CHO's with repeated data quality issues will be provided with increasing levels of support to assist in resolving data issues. Support may include additional training and/or technical assistance from the HMIS Lead.

If increased support does not result in the CHO meeting data quality standards, the CHO may be required to submit a corrective action plan to the HMIS Lead and to provide regular reports to the HMIS Lead on progress toward implementing the identified corrective actions.

Components of a corrective action plan may include:

- Developing and following a schedule of actions for carrying out HMIS-related tasks, including schedules, timetables, and milestones.
- Establishing and following an HMIS data quality plan that assigns responsibilities for carrying out remedial actions.
- Increased monitoring and reporting of HMIS data quality.

## **SECTION 5: COMPLIANCE AND TECHNICAL ASSISTANCE**

---

The goal of the CoC and the HMIS Lead is to ensure that CHOs comply with all requirements and are using HMIS to improve services to participants. If CHOs have difficulty achieving compliance, the HMIS Lead will provide technical assistance, as necessary.

CHOs are subject to annual HMIS monitoring. If compliance issues are identified through monitoring, the HMIS Administrator will assist the CHO in developing a plan for coming into compliance, and the Administrator will monitor progress toward meeting requirements of the plan.

Compliance with the policies and procedures set forth in this manual and the level of data quality achieved will be reported to the CoC Review and Ranking Committee, which takes these factors into consideration when evaluating new and renewal project applications in the annual CoC funding competition.

## SECTION 6: SECURITY PLAN

---

### Security Officers

The Cape Cod and Islands CoC has designated the HMIS Lead as the HMIS Security Officer. The duties include:

- Review of the Security Plan annually or anytime there is a change to the security management process, software, methods of data exchange, and any HMIS data or technical requirements issued by HUD. If changes are required to the HMIS Security Plan, the Security Officer will work with the HMIS Committee for review, modification, and approval.
- Confirmation that the Cape Cod and Islands CoC HMIS adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the Cape and Islands CoC HMIS and communication of security related HMIS information to CHOs.

### Identification of CHO HMIS Security Officer

Each CHO must also designate a CHO HMIS Security Officer ([Appendix 8](#)) whose duties include:

- Confirmation that the CHO adheres to the Security Plan.
- Communication of any security questions, requests, or security breaches to the Cape Cod and Islands CoC HMIS Security Officer, and security related HMIS information relayed from the Cape Cod and the Islands HMIS System Administrator to the CHO's end users.
- Participation in security training offered by the Cape Cod and Islands CoC, which is mandatory and conducted annually.

### Annual Security Certification

The Cape Cod and Islands CoC and each CHO must complete an annual security review to ensure the implementation of the security requirements for the HMIS. This security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan. If the requirement cannot be met at the time of the initial certification, the Security Officer must indicate a date not later than three months after the initial certification by which the requirement will have been met. At that time, the Security Officer will be required to submit an updated version of this form demonstrating compliance. All CHO Security Officers must complete the Security Compliance Certification ([Appendix 9](#)) and submit the completed form to the CoC Security Officer no later than July 1 of each year.

### Security Awareness Training and Follow-up

All users of the HMIS must complete security and privacy training prior to receiving a username and password and accessing the system. The End User agreement requires verification that the user has completed the on-line security training. CHOs that do not participate in the CoC's HMIS platform should confirm in writing to the HMIS Administrator that staff who have access to data that will be uploaded to the CoC's HMIS have completed the online security training. In addition, the Cape Cod and Islands CoC shall provide annual security training.

### Reporting Security Incidents

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

#### Security Incidents

All HMIS users are obligated to report to their agency HMIS Security Officer suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion as soon as such breaches are discovered. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the Cape Cod and Islands HMIS software to the HMIS Lead as soon as such incidents are reported to them. The HMIS Lead will report such incidents to the Cape & Islands Regional Network on Homelessness Executive Committee.

#### Reporting Process

HMIS users will report security violations to their CHO HMIS Security Officer, who in turn will report violations to the HMIS System Administrator. Any security breaches identified by the HMIS software vendor will also be communicated to the System Administrator. End users who violate privacy or confidentiality standards will be referred to the HMIS System Administrator for additional data security training. The HMIS Administrator will review violations and recommend corrective actions as appropriate. Serious or ongoing lapses of data security or violations of the CoC Data Security policies may result in the revocation of the end user's HMIS license and the permanent de-activation of the user's HMIS account. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

#### Audit Controls

The HMIS software vendor maintains an accessible audit trail within the system that allows the HMIS Administrator to monitor user activity and examine data access for specified users. The HMIS Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures.

## System Security

Each CHO must apply system security provisions to all the systems where PII is collected or stored, including, but not limited to, a CHO's networks, desktops, laptops, mini- computers, mainframes, and servers.

### User Authentication

A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

### Virus Protection

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

### Firewalls

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall if there is a firewall between that workstation and any outside systems, including the Internet and other computer networks. For example, a workstation that accesses the Internet through a modem needs its own firewall. A workstation that accesses the Internet through a central server does not need a firewall if the server has a firewall.

### Physical Access to Systems with Access to HMIS Data

A CHO must ensure that computers stationed in public areas that are used to collect and store HMIS data are staffed at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. Workstations should automatically turn on a password protected screen saver when the workstation is temporarily idle. If staff leave a workstation, even for a moment, they should log off the system. If leaving for an extended period of time, they should log off and shut down the computer.

### Hard Copy Security

A CHO must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to, reports, data entry forms, and signed consent forms. A CHO must always supervise any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO's place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying, or printing all documents containing PII should be removed from the machines promptly.

### Electronic Communication

All electronic communications containing PII retrieved from the HMIS or collected and stored in hard copy format for entry into HMIS must be sent via encrypted email. No client-level HMIS data may be sent electronically unless the transmission is secured through encryption.



### Database Integrity

The CHO must not intentionally cause corruption of the Cape Cod and Island HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information or interference with normal system operations will result in immediate suspension of HMIS licenses held by the CHO and suspension of continued access to the Cape Cod and Islands HMIS by the CHO.

The Cape Cod and Islands CoC will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to corrective actions as described in this HMIS Policies and Procedures Manual.

### Disaster Recovery

Cape Cod and Islands CoC HMIS data must be stored by the HMIS software vendor in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS Administrator will coordinate with the vendor to ensure the HMIS is operational and that data is restored. The Cape Cod and Islands CoC will communicate to CHOs when data becomes accessible following a disaster. The WellSky Disaster Recovery plan may be found in [Appendix 10](#).

### Contracts and other arrangements

Barnstable County, as HMIS Lead Entity, shall retain copies of all CHO Participation Agreements executed as part of the administration and management of the CoC's HMIS and/or necessary to comply with HUD requirements. Barnstable County shall also retain copies of the contract and data sharing agreement executed between the CoC and the MA Department of Housing and Community Development (DHCD), as Administrator of the MA Rehousing Data Collective, in which the Cape Cod and Islands CoC participates.

## SECTION 7: PRIVACY PLAN AND NOTICE SIGN

---

### Data Collection Notice

Agencies that contribute HMIS data must let clients know that PII is being collected and why it is being collected. A sample data collection notice may be found in [Appendix 11](#). The sample sets forth the explanatory language in English and Spanish and may be posted to meet the notice requirement. While the posted notice is the minimum requirement, agencies may choose to take additional steps to obtain consent from clients, including obtaining written consent.

### Privacy Notice

Each agency is required to publish and post on its web site a Privacy Notice describing its policies and practices for use of protected personal information and must provide a copy of its Privacy Notice to any individual upon request. The agency must post a sign stating the availability of its Privacy Notice to any individual who requests a copy. Sample Privacy Notices may be found in [Appendix 12](#) (English) and [Appendix 13](#) (Spanish). These documents may be used as is or adapted to each specific agency.

### Accountability

Agencies must require staff to sign an agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice. A CHO must establish a written policy for accepting and considering questions or complaints about its privacy and security policies and practices.

### Access and Correction

In general, agencies must allow an individual to inspect and to have a copy of any information about the individual and must offer to explain any information that the individual may not understand. Agencies must consider any request by an individual for correction of inaccurate or incomplete information about the individual but is not required to remove any information. However, the agency may mark information as inaccurate or incomplete and may supplement it with additional information.

The agency may deny access to personal files for any of the following reasons, and should describe reasons in its Privacy Notice:

1. Information compiled in reasonable anticipation of litigation
2. Information about another individual
3. Information obtained under a promise of confidentiality if disclosure would reveal

- the source of the information
4. Information, the disclosure of which would be likely to endanger the life or physical safety of any individual.

The agency can reject repeated or harassing requests for access or correction. An agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

## Purpose and Use Limitations

Agencies may use or disclose PII from HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions; or (4) for creating de-identified PII.

Certain disclosures may be required due to provider obligations that go beyond the privacy interests of clients. The following additional uses and disclosures are recognized by HUD, and the HMIS Lead may provide additional guidance regarding these circumstances (each of which is described in more detail in the HUD 2004 HMIS Technical Standards):

1. Uses and disclosures required by law
2. Uses and disclosures to avert a serious threat to health or safety
3. Uses and disclosures about victims of abuse, neglect, or domestic violence
4. Uses and disclosures for academic research purposes
5. Disclosures for law enforcement purposes

## Confidentiality

Each agency must develop and implement written procedures to ensure: (1) All records containing protected Identifying information of any individual or family who applies for and/or receives Continuum of Care assistance will be kept secure and confidential; (2) The address or location of any family violence project assisted with Continuum of Care funds will not be made public, except with written authorization of the person responsible for the operation of the project; and (3) The address or location of any housing of a program participant will not be made public, except as provided under a preexisting privacy policy of the recipient or subrecipient and consistent with State and local laws regarding privacy and obligations of confidentiality.

## Protections for victims of domestic violence, dating violence, sexual assault, and stalking

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients include explicit training for staff handling PII of the potentially dangerous circumstances that may be created by improper release of this information.

## Other Requirements

All agencies that contribute HMIS data must comply with the baseline privacy requirements described in this Privacy Plan. A CHO must comply with federal, state, and local laws that require additional confidentiality protections. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must contact the Cape Cod and Islands HMIS Administrator and collaboratively update the applicable policies for the CHO to accurately reflect the additional protections.

## Certain Protected Health Information

When agencies collect certain types of information about clients, the government requires that data to be protected. Information that includes references to substance use, a diagnosis of substance use disorder, or treatment for substance use disorder; diagnosis, treatment, or referrals related to a mental health disorder or HIV/AIDS, including progress notes and psychotherapy notes; and domestic violence concerns may not be shared with other participating Agencies without the clients' written consent, unless otherwise permitted by law (see [Appendix 14](#)).

## APPENDIX 1: MA-503 CoC HMIS PARTICIPATION AGREEMENT



### MA-503 CAPE COD AND ISLANDS CONTINUUM OF CARE - HMIS PARTICIPATION AGREEMENT

This agreement is entered into on \_\_\_\_\_ (date) between Barnstable County, hereafter known as "the HMIS Lead" and \_\_\_\_\_ (agency name), hereafter known as the "Contributing HMIS Organization" or "CHO," regarding access and use of the Cape Cod and Islands Continuum of Care (CoC) Homeless Management Information System, hereafter known as "HMIS."

#### I. Introduction

HMIS is a shared human services database that allows authorized personnel at homeless and human service provider agencies throughout Cape Cod and Islands CoC to enter, track, and report on information concerning their own clients and to share information, subject to appropriate inter-agency agreements, on common clients. The goals for HMIS are to:

- Improve coordinated care for and services to homeless participants in Cape Cod and Islands CoC
- Provide a user-friendly and high-quality automated records system that expedites client intake procedures, improves referral accuracy, and supports the collection of quality information that can be used for program improvement and service-planning
- Meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD) and other funders as needed

In compliance with all state and federal requirements regarding client confidentiality and data security, the HMIS is designed to collect and deliver timely, credible, quality data about services and homeless participants or participants at risk for being homeless. The Cape Cod and Islands CoC has selected WellSky's Servicepoint / Community Services as its HMIS application. HMIS will be administered by the HMIS Lead.

#### II. HMIS Lead Responsibilities

1. The HMIS Lead will offer the CHO 24-hour secure access to HMIS, via a secure CHO-provided internet connection.
2. The HMIS Lead will provide model Data Collection notices, Privacy Notices, Client Release forms and other templates for agreements that may be adopted or adapted in the CHO's implementation of HMIS functions.
3. The HMIS Lead will provide both initial training and periodic updates to that training for core CHO staff regarding the use of HMIS, with the expectation that the CHO will take responsibility for conveying this information to all designated CHO staff using the system.

4. To the extent required by its agreements with WellSky's Servicepoint/Community Services (the HMIS software vendor), the HMIS lead will coordinate with the software vendor in providing basic user support and technical assistance (i.e., general troubleshooting and assistance with standard report generation) to the designated Agency Administrator. Access to this basic technical assistance will be available in accordance with agreements between CoC and the vendor. It is expected, but not required, that such basic technical assistance will normally be available from 8:00 a.m. to 4:00 p.m. Monday through Friday (with the exclusion of holidays).
5. The HMIS Lead will not publish reports that identify specific participants/clients or provide any protected information in an identifiable format, unless otherwise required by law. Public reports will be limited to presentation of de-identified aggregated data within the HMIS database.
6. The publication practices of the HMIS Lead will be governed by policies established by the CoC.

### III. CHO Responsibilities

1. The CHO Executive Director or authorized signatory will designate a CHO HMIS Agency Administrator who will be the liaison between the HMIS Lead and the CHO. The Agency Administrator will report issues via email to the HMIS lead and assume responsibility for providing ongoing user support to all users within the CHO, including but not limited to the training of any staff person prior to issuance of a user account.
2. The CHO will enter all minimum required data elements as defined for all participants who are participating in services funded by the U.S. Department of Housing and Urban Development (HUD) Continuum of Care (CoC) Program, Emergency Shelter Grant (ESG) Program, or Housing Opportunities for Participants with AIDs (HOPWA). The CHO will enter data in a consistent manner and will strive for real-time, or close to real-time, data entry.
3. The CHO will routinely review records it has entered into HMIS for completeness and data accuracy. The review and data correction process will be made according to the MA-503 Cape Cod and Islands CoC HMIS Policies and Procedures Manual ("Policies and Procedures Manual").
4. The CHO will not knowingly enter inaccurate or false information into HMIS.
5. The CHO will review and assess data entered into HMIS and will enter data revisions as necessary to reflect a change in the status of an applicant for, or a recipient of, benefits or services, enter updates, or edit incorrect information.
6. The CHO will utilize the HMIS for official purposes only.
7. The CHO will keep updated virus protection software on the computers it uses to access the HMIS.
8. The use, disclosure and/or transmission of material in violation of any Federal or State law or regulations is prohibited.
9. The CHO will not use HMIS with intent to defraud the Federal, State, County, or local government, or an individual entity, or to conduct any illegal activity.



10. The CHO agrees to designate one specific staff member to regularly attend Cape & Islands Regional Network on Homelessness meetings and other local or regional user meetings to discuss procedures, updates, policy and practice guidelines, data analysis, and software/ hardware upgrades.
11. The CHO agrees to abide by the Policies and Procedures Manual along with any other policies and procedures that the HMIS Lead or the Cape Cod and Islands CoC publishes from time to time.

#### **IV. Privacy and Confidentiality**

##### ***A. Protection of Client Privacy***

1. The CHO will comply with all applicable federal, state, and local laws, or any superseding law or executive order, regarding protection, security, and confidentiality of client privacy.
2. The CHO will comply specifically with Federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records.
3. The CHO will comply specifically with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services, as currently in effect.
4. The CHO will dispose of all applicable records in compliance with G.L. c. 93I, applicable records retention requirements, and HIPAA.
5. The CHO will comply with applicable data privacy and security requirements, including HIPAA's Privacy Rule, 45 CFR [Part 160](#) and Subparts A and E of [Part 164](#), and G.L. c. 93H, and G.L. c. 93I.
6. The CHO will comply with all policies and procedures established by the Cape Cod and Islands CoC HMIS Lead pertaining to confidentiality, security and protection of client privacy and records.

##### ***B. Client Confidentiality***

1. The CHO agrees to post a data collection sign that meets the requirements of the Policies and Procedures Manual at all intake locations. The CHO will also make available the Cape and Islands CoC HMIS Privacy Notice to each consumer and post the Privacy Notice on the CHO's website. The CHO will provide a verbal explanation of HMIS and arrange for a qualified interpreter/translator for any individuals who need translation assistance with the Data Collection notice, the Privacy Notice, or the Release of Protected Information.
2. The CHO will not solicit or enter information from clients into HMIS unless it is essential to provide services, report to CHO funders, or conduct evaluations or research.

3. The CHO will not divulge any confidential information received from HMIS to any organization or individual without proper written consent by the client, unless otherwise permitted or required by applicable regulation or law.
4. The CHO will ensure that all participants who are issued a User Identification and Password to HMIS abide by this Participation Agreement, including all associated confidentiality provisions. The CHO will be responsible for oversight of its own related confidentiality requirements.
5. The CHO agrees that it will not request a User ID and Password for any person until the individual completes the HMIS Lead's online Privacy and Security training module.
6. The CHO acknowledges that ensuring the confidentiality, security, and privacy of any information downloaded from the system by the CHO is strictly the responsibility of the CHO.
7. The CHO agrees that it will establish a procedure for accepting and considering questions or complaints about its privacy and security policies and procedures.

#### ***C. Sharing of Client Information***

1. The CHO acknowledges that all forms provided by Cape Cod and Islands CoC HMIS regarding client privacy and confidentiality are shared with the HMIS Lead as generally applicable models that may require modification in accord with CoC-specific rules. The CHO may revise (as necessary) all forms provided by the HMIS lead to assure that they are in compliance with the laws, rules, and regulations that govern its organization, but in no case shall the CHO relax any confidential rules established by this Participation Agreement or any other Cape Cod and Islands CoC HMIS policy or procedure.
2. The CHO acknowledges that informed client consent is required before client information is entered into the system. The CHO will document client consent prior to entering client data into the HMIS.
3. The CHO will obtain additional written consent through a RELEASE OF PROTECTED INFORMATION if the CHO intends to share Protected Client Data, as so defined, within the HMIS. Restricted information about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, including progress notes and psychotherapy notes, and domestic violence concerns shall not be shared with other participating Agencies without the client's written, informed consent as documented above.
4. The CHO acknowledges that the CHO, itself, bears primary responsibility for oversight for all sharing of data it has collected via the HMIS. The CHO agrees to place all signed RELEASES OF PROTECTED INFORMATION forms in a file at the CHO's business address and that such forms will be made available to the HMIS Lead for periodic audits. The CHO will retain these forms in compliance with applicable record retention requirements, after which time the forms will be securely destroyed in a manner that ensures client confidentiality is not compromised.



5. The CHO acknowledges that clients who choose not to authorize the disclosure of Protected Information cannot be denied services for which they would otherwise be eligible.

#### ***D. Custody of Data***

1. The CHO acknowledges, and the Cape Cod and Islands CoC agrees, that the CHO retains ownership over all information it enters into HMIS.
2. If the Cape Cod and Islands CoC HMIS ceases to exist, the CHO will be notified and provided reasonable time to securely access and save client data as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.
3. If the Cape Cod and Islands CoC ceases to exist, or Barnstable County ceases its service as the CoC's HMIS Lead, the custodianship of the data within HMIS will be securely transferred by the HMIS Lead to another organization for continuing administration, and the CHO will be informed in a timely manner.

#### **V. Publication of Reports**

1. The CHO agrees that it may only release de-identified aggregated information generated by HMIS that is specific to its own services, unless otherwise authorized by law.
2. The CHO acknowledges that the release of de-identified aggregated information will be governed through policies established by the Continuum of Care.

#### **VI. Database Integrity and Sanctions**

1. The CHO will comply with the security standards set forth in the HUD HMIS standards, the Policies and Procedures Manual, and the Cape Cod and Islands CoC HMIS Security Plan, including establishment of mechanisms to protect and secure electronic and hardcopy data. The CHO will not share assigned User IDs and Passwords to access HMIS with any other organization, governmental entity, business, or individual, unless required by law.
2. The CHO will not intentionally cause corruption of HMIS data in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of services, and, where appropriate, legal action against the offending entities and/or disciplinary action against employees.
3. The CHO will thoroughly investigate all potential violations of any security protocols. Any user or CHO found to be in violation of security protocols will be sanctioned. Sanctions may include, but are not limited to:
  - a. Suspending or terminating access to HMIS
  - b. Suspending funds disbursement
  - c. Reducing or terminating the remaining grant
  - d. Imposing conditions on future grants
  - e. Imposing other legally available remedies

4. The CHO's access may be suspended or revoked for serious or repeated violations of HMIS Policies and Procedures by CHO users. CHOs that lose the ability to access and contribute data to HMIS may not receive CoC Program or ESG funding.

## **VII. Hold Harmless**

1. The HMIS Lead makes no warranties, expressed or implied. To the extent permitted by law, the CHO, at all times, will indemnify and hold the HMIS Lead harmless from any damages, liabilities, claims, and expenses that may be claimed against the CHO; or for injuries or damages to the CHO or another party arising from participation in the HMIS; or arising from any acts, omissions, neglect, or fault of the CHO or its agents, employees, licensees, or clients; or arising from the CHO's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. The CHO will also hold the Cape Cod and Islands CoC and HMIS Lead harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by WellSky, by the CHO's or other CHOs' negligence or errors or omissions, as well as natural disasters, technological difficulties, and/or acts of God. The HMIS Lead shall not be liable to the CHO for damages, losses, or injuries to the CHO or another party other than if such is the result of gross negligence or willful misconduct of the HMIS Lead.
2. The CHO agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than five hundred thousand dollars (\$500,000), to include coverage for the CHO's indemnification obligations under this agreement.
3. Provisions of Section VII shall survive any termination of the Participation Agreement.

## **VIII. Terms and Conditions**

1. The parties hereto agree that this Participation Agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. Neither party shall assign or transfer its rights, responsibilities, or obligations under this Participation Agreement.
3. This agreement shall remain in force until revoked in writing by either party, with 30 days' advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breaches of this agreement. Should such situations arise, the HMIS Lead may immediately suspend access to HMIS until the allegations are resolved to protect the integrity of the system.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days' advance written notice.
5. The parties agree that Cape Cod and Islands CoC is a third-party beneficiary of this contract and may enforce the terms and provisions of this contract as applicable.

6. If any provision of this Participation Agreement shall be held invalid or unenforceable, it shall not affect the validity or enforceability of the remainder of this Participation Agreement.

7. This Participation Agreement shall be governed by, construed, and enforced in accordance with the laws of the Commonwealth of Massachusetts. All parties hereby agree to the jurisdiction of the courts of the Commonwealth of Massachusetts with respect to any legal proceedings arising out of this Agreement, and further agree to Springfield, Massachusetts as the place of venue for any such action.

8. IN WITNESS WHEREOF, the parties have entered into this Participation Agreement:

CHO: \_\_\_\_\_

Address: \_\_\_\_\_

Name and Title of Authorized Signatory: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**HMIS LEAD: Barnstable County Department of Human Services**

Name and Title of Authorized Signatory: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## APPENDIX 2: DESIGNATION OF AGENCY ADMINISTRATOR



### MA-503 CAPE COD AND ISLANDS CoC HOMELESS MANAGEMENT INFORMATION SYSTEM

#### DESIGNATION OF HMIS AGENCY ADMINISTRATOR

I, the undersigned, certify that I am the executive director, or other chief executive officer, of the below-named agency and that I have legal authority to sign legally binding documents on behalf of the below-named agency. I hereby designate the individual named below to complete all HMIS Agency Administrator duties as described in the HMIS Participation Agreement between the Cape Cod and Islands CoC and the Agency.

---

Agency name

---

Agency address

City

State

Zip

---

Signature of executive director or other chief executive officer

Date signed

---

Printed name and exact title of executive director or other chief executive officer

---

Printed name and title of Agency Administrator

---

Agency Administrators' phone number

Agency Administrator's fax number

---

Agency Administrators' email address

## APPENDIX 3: HMIS END USER AGREEMENT



### MA-503 CAPE COD AND ISLANDS CONTINUUM OF CARE HOMELESS MANAGEMENT INFORMATION SYSTEM – END USER AGREEMENT

Agency Name \_\_\_\_\_

Employee/End User Name \_\_\_\_\_

The MA-503 Cape Cod and Islands Continuum of Care Homeless Management Information System ("HMIS") is a collaborative project with participating homeless shelter and service providers in the Cape Cod and Islands Continuum of Care ("CoC") region. HMIS enables homeless service providers to collect uniform client information over time. This system is essential to efforts to streamline client services and inform public policy. Analysis of information gathered through HMIS is critical to accurately calculate the size, characteristics, and needs of the homeless population. This data is also necessary for service and systems planning.

The HMIS project recognizes the diverse needs and vulnerability of the homeless community. The goal of HMIS is to improve the coordination of care for homeless and at-risk individuals and families in the region. It is important that client confidentiality is vigilantly maintained and that we treat the personal data of our most vulnerable populations with respect and care.

As the holders of this personal data, HMIS users have an ethical and legal obligation to ensure that they collect, access, and use client data appropriately and in compliance with applicable legal requirements. It is also the responsibility of each user to ensure that he or she uses client data only for the purposes outlined in the MA-503 Cape Cod and Islands Continuum of Care HMIS Policies and Procedures Manual ("Policies and Procedures Manual").

Your username and password will allow you to access HMIS. Initial each item below to indicate that you understand the proper use of your username and password and that you agree to abide by the Policies and Procedures Manual.

\_\_\_\_\_ I have received training on how to use HMIS and have completed the required HMIS Data Security and Confidentiality training.

\_\_\_\_\_ I understand and agree that my username and password are for my use only and may not be shared with anyone. I must take all reasonable means to keep my password physically secure.

**I HAVE CHECKED EACH BOX TO INDICATE THAT I UNDERSTAND AND AGREE TO COMPLY WITH THE STATEMENTS BELOW.**

☐ I understand and agree that the only individuals who can view HMIS information are authorized users and the clients to whom the information pertains.



- ☐ I understand and agree that I may only view, obtain, disclose, and use the database information that is necessary to perform the essential functions of my position in compliance with legal and policy requirements.
- ☐ I understand and agree that if I am logged into HMIS and must leave the work area where the computer is located for any period of time, I must log-off the system before leaving the work area. Failure to do so may result in a breach of client confidentiality and system security and may result in employee discipline.
- ☐ I understand and agree that these rules apply to all users of HMIS, whatever their work role or position.
- ☐ I understand and agree that all HMIS information (hard copies and soft copies) must be kept secure and confidential at all times, and when no longer needed, they must be properly destroyed to maintain confidentiality, in accordance with legal requirements, including, but not limited to, the applicable Records Retention Requirements.
- ☐ I understand and agree that if I notice or suspect a security breach within HMIS, I must immediately notify my Agency Administrator.
- ☐ I understand and agree that I will not knowingly enter malicious or erroneous information into HMIS.
- ☐ I understand and agree that any questions or disputes about the data entered by another agency should be directed to the System Administrator.
- ☐ I understand that in the event I am no longer an employee of the Agency, or the Agency has determined in its sole discretion that access is no longer justified or needed, my access to HMIS will be revoked.
- ☐ I understand that I will share PROTECTED INFORMATION\* of only those clients who have signed the HMIS Release of Information or otherwise authorized or required by law.
- ☐ I understand and agree to attend Cape Cod and Islands CoC HMIS End User Training and other period trainings offered by the System Administrator.
- ☐ I understand and agree to maintain strict confidentiality of information obtained through the Cape Cod and Islands CoC HMIS. This information will be used only for the legitimate client service and administration of the agency. Any breach of confidentiality will result in immediate termination of participation in HMIS, as well as potential employee discipline, up to and including termination, in addition to any other applicable legal penalties.

*\*PROTECTED INFORMATION is information that includes medical information, including references to substance use, a diagnosis of substance use disorder, or treatment for substance use disorder; diagnosis, treatment, or referrals related to a mental health disorder or HIV/AIDS, including progress notes and psychotherapy notes; and domestic violence concerns.*

Employee/End User Signature \_\_\_\_\_ Date \_\_\_\_\_

Agency Administrator Signature \_\_\_\_\_ Date \_\_\_\_\_

## APPENDIX 4: DATA COLLECTION TEMPLATES – CLIENT RECORD, DEMOGRAPHICS, PROJECT ENTRY ASSESSMENT

MA-503 CAPE COD AND ISLANDS CoC - HMIS CLIENT DATA ENTRY	
AGENCY NAME <input style="width: 100%;" type="text"/>	PROJECT NAME NAME <input style="width: 100%;" type="text"/>
PROJECT ENTRY DATE <input style="width: 100%;" type="text"/>	
CLIENT RECORD	CLIENT DEMOGRAPHICS
<p>FIRST NAME <input style="width: 100%;" type="text"/></p> <p>MIDDLE NAME <input style="width: 100%;" type="text"/></p> <p>LAST NAME <input style="width: 100%;" type="text"/></p> <p>SUFFIX</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Jr.  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Sr.  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> I  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> II  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> III  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> IV         </div> <p>NAME DATA QUALITY</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Full name reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Partial name reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div> <p>SOCIAL SECURITY <input style="width: 100%;" type="text"/></p> <p>SSN DATA QUALITY</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Full SSN reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Partial SSN reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div> <p>US VETERAN?</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Yes  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> No  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div>	<p>DATE OF BIRTH <input style="width: 100%;" type="text"/></p> <p>DoB TYPE</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Full DoB reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Partial DoB reported  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div> <p>GENDER</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Female  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Male  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Non-binary / Gender Fluid  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Transgender  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Questioning  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div> <p>PRIMARY RACE</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> American Indian, Native Alaskan, Indigenous  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Asian, Asian American  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Black, African American, African  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Native Hawaiian, Pacific Islander  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> White  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div> <p>SECONDARY RACE</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> American Indian, Native Alaskan, Indigenous  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Asian, Asian American  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Black, African American, African  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Native Hawaiian, Pacific Islander  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> White         </div> <p>ETHNICITY</p> <div style="display: flex; align-items: center;"> <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Hispanic/Latin(a)(o)(x)  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Non-Hispanic/Non-Latin(a)(o)(x)  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Doesn't know  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Refused  <input style="width: 20px; height: 20px; margin-right: 5px;" type="checkbox"/> Data not collected         </div>

## MA-503 CAPE COD AND ISLANDS CoC - HMIS PROJECT ENTRY ASSESSMENT (1)

CLIENT NAME

PROJECT ENTRY DATE

 /  / 

RELATIONSHIP TO HoH

- ☐ Self (HoH)
- ☐ HoH's child
- ☐ HoH's spouse or partner
- ☐ HoH's other relation
- ☐ Other: non-relation
- ☐ Data not collected

DOES CLIENT HAVE DISABLING CONDITION?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

DATE OF BIRTH

 /  / 

DATE OF BIRTH TYPE

- ☐ Full DoB reported
- ☐ Partial DoB reported
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

DISABILITIES

- ☐ Alcohol Use Disorder
- ☐ Both Drug and Alcohol Use
- ☐ Chronic Health Condition
- ☐ Developmental Disability
- ☐ Drug Use Disorder
- ☐ HIV / AIDS / HEP C
- ☐ Mental Health Condition
- ☐ Physical Disability

GENDER

- ☐ Female
- ☐ Male
- ☐ Non-binary/gender fluid
- ☐ Questioning
- ☐ Transgender
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

HEALTH INSURANCE

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

PRIMARY RACE

- ☐ American Indian, Alaska Native, Indigenous
- ☐ Asian, Asian American
- ☐ Black, African American, African
- ☐ Native Hawaiian, Pacific Islander
- ☐ White
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

HEALTH INSURANCE TYPE

- ☐ MEDICAID (MassHealth)
- ☐ MEDICARE
- ☐ State CHIP
- ☐ VA Medical Insurance
- ☐ Employer Provided
- ☐ COBRA
- ☐ Private Pay
- ☐ State Insurance for Adults
- ☐ Indian Health Services
- ☐ Other

SECONDARY RACE

- ☐ American Indian, Alaska Native, Indigenous
- ☐ Asian, Asian American
- ☐ Black, African American, African
- ☐ Native Hawaiian, Pacific Islander
- ☐ White

CLIENT LOCATION CODE

 MA-503

ETHNICITY

- ☐ Hispanic/Latin(a)(o)(x)
- ☐ Non-Hispanic/Non-Latin(a)(o)(x)
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

PRIOR LIVING SITUATION

HOMELESS SITUATIONS

- ☐ Place not meant for habitation
- ☐ ES / Motel with voucher
- ☐ Safe haven

INSTITUTIONAL SITUATIONS

- ☐ Foster care / group home
- ☐ Hospital (non psychiatric)
- ☐ Jail/prison/juvenile detention
- ☐ Long term care/nursing home
- ☐ Psychiatric hospital
- ☐ Substance abuse facility/detox



# MA-503 CAPE COD AND ISLANDS CoC - HMIS PROJECT ENTRY ASSESSMENT (2)

CLIENT NAME  PROJECT ENTRY DATE  /  /

## PRIOR LIVING SITUATION (CONTINUED)

### TEMPORARY/PERMANENT HOUSING

- ☐ Halfway house
- ☐ Motel / no voucher
- ☐ Transitional housing
- ☐ Host home (non-crisis)
- ☐ Friends
- ☐ Family
- ☐ Rental with GDP TIP
- ☐ Rental with VASH
- ☐ PH (non-RRH) dedicated
- ☐ Rental RRH
- ☐ Rental with HCV
- ☐ Rental in public housing
- ☐ Rental with no subsidy
- ☐ Rental with other subsidy
- ☐ Owned with subsidy
- ☐ Owned with no subsidy

### OTHER

- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

TOWN OF PRIOR LIVING SITUATION

### LENGTH OF STAY IN PRIOR LIVING SITUATION

- ☐ One night or less
- ☐ Two to six nights
- ☐ One week or more but less than one month
- ☐ One month or more but less than 90 days
- ☐ 90 days or more but less than one year
- ☐ One year or longer
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

ON THE NIGHT BEFORE, DID YOU STAY UNSHELTERED, ES, SH?

- ☐ Yes
- ☐ No

IF YES: DATE HOMELESSNESS STARTED  /  /

### NUMBER OF TIMES HOMELESS PAST 3 YEARS

- ☐ One time
- ☐ Two times
- ☐ Three times
- ☐ Four or more times
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

## IF YES (CONTINUED):

### NUMBER OF MONTHS HOMELESS IN PAST 3 YEARS

- ☐ 1 (this is the first time)
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7
- ☐ 8
- ☐ 9
- ☐ 10
- ☐ 11
- ☐ 12
- ☐ More than 12
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### INCOME FROM ANY SOURCE

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### SOURCE

- ☐ Alimony
- ☐ Child support
- ☐ Earned Income
- ☐ General Assistance
- ☐ Other
- ☐ Pension
- ☐ Private disability
- ☐ SS Retirement
- ☐ SSDI
- ☐ SSI
- ☐ TANF
- ☐ Unemployment
- ☐ VA Non-service disability
- ☐ VA service disability
- ☐ Workers comp

MONTHLY AMOUNT \$

### NON-CASH BENEFITS

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### SOURCE

- ☐ SNAP
- ☐ WIC
- ☐ TANF Child Care
- ☐ TANF Transportation
- ☐ Other TANF Services
- ☐ Other Source

## APPENDIX 5: PROJECT ANNUAL / UPDATE ASSESSMENTS

MA-503 CAPE COD AND ISLANDS CoC - ANNUAL/UPDATE ASSESSMENT (1)	
CLIENT NAME <input style="width: 90%;" type="text"/>	ASSESSMENT DATE <input style="width: 10%;" type="text"/> / <input style="width: 10%;" type="text"/> / <input style="width: 10%;" type="text"/>
<b>HEALTH INSURANCE</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>HEALTH INSURANCE TYPE</b> <input type="checkbox"/> MEDICAID (MassHealth) <input type="checkbox"/> MEDICARE <input type="checkbox"/> State CHIP <input type="checkbox"/> VA Medical Insurance <input type="checkbox"/> Employer Provided <input type="checkbox"/> COBRA <input type="checkbox"/> Private Pay <input type="checkbox"/> State Insurance for Adults <input type="checkbox"/> Indian Health Services <input type="checkbox"/> Other <b>DOES CLIENT HAVE DISABLING CONDITION?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>DISABILITIES</b> <input type="checkbox"/> Alcohol Use Disorder <input type="checkbox"/> Both Drug and Alcohol Use <input type="checkbox"/> Chronic Health Condition <input type="checkbox"/> Developmental Disability <input type="checkbox"/> Drug Use Disorder <input type="checkbox"/> HIV / AIDS / HEP C <input type="checkbox"/> Mental Health Condition <input type="checkbox"/> Physical Disability <b>CLIENT LOCATION CODE</b> <input style="width: 100%;" type="text" value="MA-503"/> <b>INCOME FROM ANY SOURCE</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>SOURCE</b> <input type="checkbox"/> Alimony <input type="checkbox"/> Child support <input type="checkbox"/> Earned Income <input type="checkbox"/> General Assistance <input type="checkbox"/> Other <input type="checkbox"/> Pension <input type="checkbox"/> Private disability <input type="checkbox"/> SS Retirement <input type="checkbox"/> SSDI <input type="checkbox"/> SSI <input type="checkbox"/> TANF <input type="checkbox"/> Unemployment <input type="checkbox"/> VA Non-service disability <input type="checkbox"/> VA service disability <input type="checkbox"/> Workers comp <b>MONTHLY AMOUNT</b> <input style="width: 100px;" type="text" value="\$"/>	<b>NON-CASH BENEFITS</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>SOURCE</b> <input type="checkbox"/> SNAP <input type="checkbox"/> WIC <input type="checkbox"/> TANF Child Care <input type="checkbox"/> TANF Transportation <input type="checkbox"/> Other TANF Services <input type="checkbox"/> Other Source <b>DOMESTIC VIOLENCE VICTIM / SURVIVOR?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>IF YES, WHEN?</b> <input type="checkbox"/> Within past three months <input type="checkbox"/> Three to six months ago <input type="checkbox"/> Six to twelve months ago <input type="checkbox"/> More than a year ago <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>IF YES, ARE YOU CURRENTLY FLEEING?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <b>CURRENT LIVING SITUATION</b> <b>HOMELESS SITUATIONS</b> <input type="checkbox"/> Place not meant for habitation <input type="checkbox"/> ES / Motel with voucher <input type="checkbox"/> Safe haven <b>INSTITUTIONAL SITUATIONS</b> <input type="checkbox"/> Foster care / group home <input type="checkbox"/> Hospital (non psychiatric) <input type="checkbox"/> Jail/prison/juvenile detention <input type="checkbox"/> Long term care/nursing home <input type="checkbox"/> Psychiatric hospital <input type="checkbox"/> Substance abuse facility/detox <b>TEMPORARY/PERMANENT HOUSING</b> <input type="checkbox"/> Halfway house <input type="checkbox"/> Motel / no voucher <input type="checkbox"/> Transitional housing <input type="checkbox"/> Host home (non-crisis) <input type="checkbox"/> Friends <input type="checkbox"/> Family <input type="checkbox"/> Rental with GDP TIP <input type="checkbox"/> Rental with VASH <input type="checkbox"/> PH (non-RRH) dedicated <input type="checkbox"/> Rental RRH <input type="checkbox"/> Rental with HCV <input type="checkbox"/> Rental in public housing <input type="checkbox"/> Rental with no subsidy <input type="checkbox"/> Rental with other subsidy <input type="checkbox"/> Owned with subsidy <input type="checkbox"/> Owned with no subsidy <b>OTHER (SPECIFY):</b> <input style="width: 150px;" type="text"/>

## MA-503 CAPE COD AND ISLANDS CoC - ANNUAL/UPDATE ASSESSMENT (2)

CLIENT NAME

ASSESSMENT DATE

WILL CLIENT HAVE TO LEAVE CURRENT LIVING SITUATION WITHIN

14 DAYS?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

IF YES:

HAS SUBSEQUENT RESIDENCE BEEN IDENTIFIED?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

DOES INDIVIDUAL OR FAMILY HAVE RESOURCES OR SUPPORT NETWORKS TO OBTAIN OTHER PERMANENT HOUSING?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

HAS THE CLIENT HAD A LEASE OR OWNERSHIP INTEREST IN A PERMANENT HOUSING UNIT IN THE LAST 60 DAYS?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

HAS THE CLIENT MOVED 2 OR MORE TIMES IN THE LAST 60 DAYS?

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

LOCATION DETAILS

## APPENDIX 6: PROJECT EXIT ASSESSMENT

MA-503 CAPE COD AND ISLANDS CoC - EXIT ASSESSMENT (1)	
CLIENT NAME <span style="border: 1px solid black; display: inline-block; width: 300px; height: 20px;"></span>	EXIT DATE <span style="border: 1px solid black; display: inline-block; width: 100px; height: 20px;"></span> / <span style="border: 1px solid black; display: inline-block; width: 50px; height: 20px;"></span> / <span style="border: 1px solid black; display: inline-block; width: 50px; height: 20px;"></span>
<b>REASON FOR LEAVING</b> <input type="checkbox"/> Completed program <input type="checkbox"/> Criminal activity / violence <input type="checkbox"/> Death <input type="checkbox"/> Disagreement with rules / persons <input type="checkbox"/> Left for housing opportunity before completing program <input type="checkbox"/> Needs could not be met <input type="checkbox"/> Non-compliance with program <input type="checkbox"/> Non-payment of rent <input type="checkbox"/> Other - Specify <span style="border: 1px solid black; display: inline-block; width: 250px; height: 20px;"></span> <input type="checkbox"/> Reached maximum time allowed <input type="checkbox"/> Unknown / disappeared	<b>HOUSING ASSESSMENT AT EXIT</b> <input type="checkbox"/> Able to maintain the housing they had at project entry <input type="checkbox"/> Without a subsidy <input type="checkbox"/> With subsidy they had at project entry <input type="checkbox"/> With ongoing subsidy acquired since project entry <input type="checkbox"/> Only with financial assistance other than subsidy <input type="checkbox"/> Data not collected <input type="checkbox"/> Moved into new housing unit <input type="checkbox"/> With ongoing subsidy <input type="checkbox"/> Without ongoing subsidy <input type="checkbox"/> Data not collected <input type="checkbox"/> Moved in with family/friends temporary <input type="checkbox"/> Moved in with family/friends permanent <input type="checkbox"/> Moved into Transitional or temporary housing <input type="checkbox"/> Client became homeless in shelter or unsheltered <input type="checkbox"/> Client went to jail / prison <input type="checkbox"/> Client died <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected
<b>DESTINATION</b> <b>HOMELESS SITUATIONS</b> <input type="checkbox"/> Place not meant for habitation <input type="checkbox"/> ES / Motel with voucher <input type="checkbox"/> Safe haven <b>INSTITUTIONAL SITUATIONS</b> <input type="checkbox"/> Foster care / group home <input type="checkbox"/> Hospital (non psychiatric) <input type="checkbox"/> Jail/prison/juvenile detention <input type="checkbox"/> Long term care/nursing home <input type="checkbox"/> Psychiatric hospital <input type="checkbox"/> Substance abuse facility/detox <b>TEMPORARY/PERMANENT HOUSING</b> <input type="checkbox"/> Halfway house <input type="checkbox"/> Motel / no voucher <input type="checkbox"/> Transitional housing <input type="checkbox"/> Host home (non-crisis) <input type="checkbox"/> Friends <input type="checkbox"/> Family <input type="checkbox"/> Rental with GDPTIP <input type="checkbox"/> Rental with VASH <input type="checkbox"/> PH (non-RRH) dedicated <input type="checkbox"/> Rental RRH <input type="checkbox"/> Rental with HCV <input type="checkbox"/> Rental in public housing <input type="checkbox"/> Rental with no subsidy <input type="checkbox"/> Rental with other subsidy <input type="checkbox"/> Owned with subsidy <input type="checkbox"/> Owned with no subsidy <b>OTHER</b> <input type="checkbox"/> No exit interview completed <input type="checkbox"/> Other: Specify <span style="border: 1px solid black; display: inline-block; width: 150px; height: 20px;"></span> <input type="checkbox"/> Deceased <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected	<b>IS CLIENT COVERED BY HEALTH INSURANCE?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>HEALTH INSURANCE TYPE</b> <input type="checkbox"/> MEDICAID (MassHealth) <input type="checkbox"/> MEDICARE <input type="checkbox"/> State CHIP <input type="checkbox"/> VA Medical Insurance <input type="checkbox"/> Employer Provided <input type="checkbox"/> COBRA <input type="checkbox"/> Private Pay <input type="checkbox"/> State Insurance for Adults <input type="checkbox"/> Indian Health Services <input type="checkbox"/> Other <b>DOES CLIENT HAVE DISABLING CONDITION?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Doesn't know <input type="checkbox"/> Refused <input type="checkbox"/> Data not collected <b>DISABILITIES</b> <input type="checkbox"/> Alcohol Use Disorder <input type="checkbox"/> Both Drug and Alcohol Use <input type="checkbox"/> Chronic Health Condition <input type="checkbox"/> Developmental Disability <input type="checkbox"/> Drug Use Disorder <input type="checkbox"/> HIV / AIDS / HEP C <input type="checkbox"/> Mental Health Condition <input type="checkbox"/> Physical Disability

## MA-503 CAPE COD AND ISLANDS CoC - EXIT ASSESSMENT (2)

CLIENT NAME

EXIT DATE  /  /

### INCOME FROM ANY SOURCE

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

#### SOURCE

- ☐ Alimony
- ☐ Child support
- ☐ Earned Income
- ☐ General Assistance
- ☐ Other
- ☐ Pension
- ☐ Private disability
- ☐ SS Retirement
- ☐ SSDI
- ☐ SSI
- ☐ TANF
- ☐ Unemployment
- ☐ VA Non-service disability
- ☐ VA service disability
- ☐ Workers comp

MONTHLY AMOUNT \$

### NON-CASH BENEFITS

- ☐ Yes
- ☐ No
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

#### SOURCE

- ☐ SNAP
- ☐ WIC
- ☐ TANF Child Care
- ☐ TANF Transportation services
- ☐ TANF Other services
- ☐ Other Source

### PSH CLIENTS ONLY

### GENERAL HEALTH STATUS

- ☐ Excellent
- ☐ Very good
- ☐ Good
- ☐ Fair
- ☐ Poor
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### CLIENT PERCEIVES THEIR LIFE HAS VALUE AND WORTH

- ☐ Strongly disagree
- ☐ Somewhat disagree
- ☐ Neither agree nor disagree
- ☐ Somewhat agree
- ☐ Strongly agree
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### CLIENT PERCEIVES THEY HAVE SUPPORT FROM OTHERS WHO WILL LISTEN TO THEIR PROBLEMS

- ☐ Strongly disagree
- ☐ Somewhat disagree
- ☐ Neither agree nor disagree
- ☐ Somewhat agree
- ☐ Strongly agree
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### CLIENT PERCEIVES THEY HAVE A TENDENCY TO BOUNCE BACK AFTER HARD TIMES

- ☐ Strongly disagree
- ☐ Somewhat disagree
- ☐ Neither agree nor disagree
- ☐ Somewhat agree
- ☐ Strongly agree
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

### CLIENT'S FREQUENCY OF FEELING NERVOUS, TENSE, WORRIED, FRUSTRATED, OR AFRAID

- ☐ Not at all
- ☐ Once a month
- ☐ Several times a month
- ☐ Several times a week
- ☐ At least every day
- ☐ Doesn't know
- ☐ Refused
- ☐ Data not collected

## APPENDIX 7: DATA QUALITY BENCHMARKS

General Principle	Specific Principle	Expected Benchmark	Monitoring Procedure Who? How often?
Coverage	All lodging and non- lodging homeless programs in the CoC report HMIS data	<ul style="list-style-type: none"> <li>- 100% Emergency shelter beds and Rapid Rehousing beds report in HMIS</li> <li>- 80% Transitional housing and permanent supportive housing report in HMIS.</li> </ul>	<ul style="list-style-type: none"> <li>- HIC provides annual report.</li> <li>- HMIS Administrator reports status quarterly to HMIS Committee.</li> </ul>
Completeness	All clients entered	<ul style="list-style-type: none"> <li>- 95% of clients have all universal data entered.</li> <li>- 95% of clients have project entry assessment completed.</li> <li>- 100% of clients qualifying for Annual assessment must have assessment completed.</li> </ul>	<ul style="list-style-type: none"> <li>- HMIS Administrator runs monthly Data Validation reports and sends to CHO's for data clean up.</li> </ul>
	Complete exit data entered	<ul style="list-style-type: none"> <li>- 95% of required exit assessments entered.</li> <li>- 95% of exits assessments contain complete exit information, including Exit Destination</li> </ul>	<ul style="list-style-type: none"> <li>- HMIS Administrator checks missing exit assessments and missing exit destinations on monthly Data Validation report.</li> </ul>
Accuracy	Accurate data entered by staff	<ul style="list-style-type: none"> <li>- 5 of the 6 records must be entered accurately.</li> </ul>	<ul style="list-style-type: none"> <li>- Annual random spot check of CHO paper files by HMIS Administrator against HMIS. Pull 6 records and look for client data in the database.</li> </ul>
Timeliness	Changing data kept up to date	<ul style="list-style-type: none"> <li>- Active clients should be reviewed by the HMIS System Administrator every 30 days.</li> </ul>	<ul style="list-style-type: none"> <li>- The HMIS Administrator will review with the CHO Agency Administrator on quarterly basis.</li> </ul>
	Data are entered soon after collected	<ul style="list-style-type: none"> <li>- Emergency Shelter clients must be entered within 24 hours of enrollment.</li> <li>- All non-Emergency Shelter clients must be entered within 48 hours of enrollment.</li> <li>- All Annual Assessments must be entered within 30 days before or after client anniversary date.</li> </ul>	<ul style="list-style-type: none"> <li>- If unable to enter with 24 hours, ES staff must notify the Agency Admin and the HMIS Admin by email with the reason why and the client's ID.</li> <li>Monthly reports to agencies via email, virtually, or in person.</li> </ul>
Consistency	Common interpretation of questions and answers	<ul style="list-style-type: none"> <li>- Data will be reviewed at the monthly data management meetings.</li> </ul>	<ul style="list-style-type: none"> <li>- The HMIS Administrator will compare aggregate data by users for same population to look for unusual patterns on a quarterly basis.</li> <li>- Inconsistencies found during the month will be noted and discussed at data management meetings.</li> </ul>
	Common knowledge of what fields to answer	<ul style="list-style-type: none"> <li>- 95% of required fields completed</li> </ul>	<ul style="list-style-type: none"> <li>- Monthly check of required fields in system – 95% of records have complete minimal fields.</li> </ul>



## APPENDIX 8: IDENTIFICATION OF CHO SECURITY OFFICER



### MA-503 CAPE COD AND ISLANDS CONTINUUM OF CARE - IDENTIFICATION OF HMIS SECURITY OFFICER

Organization Name \_\_\_\_\_

Security Officer Name \_\_\_\_\_

Title \_\_\_\_\_

Phone \_\_\_\_\_

Email \_\_\_\_\_

Security Officer duties include, but are not limited to:

- Annually review the Security Certification document and test the CHO security practices for compliance.
- Using this Security Certification document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time. Communicate any security questions, requests, or security breaches to the Cape Cod and Islands HMIS System Lead and Security Officer.
- Communicate security related HMIS information to the organization's end users.
- Complete security training offered by the HMIS Lead.
- Additional duties specified in the HMIS Participation Agreement.

**CHO Security Officer signature indicating understanding and acceptance of these duties:**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

## APPENDIX 9: SECURITY COMPLIANCE SELF-CERTIFICATION

MA-503 Cape Cod and Islands CoC HMIS – Annual Security Compliance Self-Certification			
Category	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
User Authentication	Does the agency abide by the HMIS policies for unique usernames and password?	<p>All HMIS users at the agency are aware that they should:</p> <p>_____Y_____N - NEVER share username and passwords</p> <p>_____Y_____N - NEVER keep usernames/ passwords in public locations</p> <p>_____Y_____N - NEVER use their internet browser to store passwords</p>	
Hard Copy Data	Does agency have procedures in place to protect hard copy PII (PPI) generated from or for the HMIS?	<p>Agency has procedure for hard copy PII that includes:</p> <p>Security of hard copy files:</p> <p>_____Y_____N - Locked drawer/file cabinet</p> <p>_____Y_____N - Locked office</p> <p>Procedure for client data generated from the HMIS:</p> <p>_____Y_____N - Printed screen shots</p> <p>_____Y_____N - HMIS client reports</p> <p>_____Y_____N - Downloaded data into Excel</p>	
Storage	<p>Does the agency dispose of or remove identifiers from a client record after a specified period of time?</p> <p>(Minimum standard: 7 years after PII was last changed if record is not in current use.)</p>	<p>_____Y_____N - Agency has a procedure</p> <p>Describe procedure: _____</p> <p>_____</p> <p>_____</p>	



Virus Protection	Do all computers have virus protection with automatic update? (This includes non-HMIS computers if they are networked with HMIS computers.)	Virus software and version	
		_____Y_____N - Auto-update turned on	
Firewall	Does the agency have a firewall on the network and/or workstation(s) to protect the HMIS systems from outside intrusion?	Single computer agencies: _____Y_____N - Individual workstation Version: _____	
		Networked (multiple computer) agencies: _____Y_____N - Network firewall	
Physical Access	Are all HMIS workstations in secure locations or are they staffed at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers.)	All workstations are: _____Y_____N - In secure locations (locked offices) or staffed at all times	
		_____Y_____N - Using password protected screensavers All printers used to print hard copies from the HMIS are: _____Y_____N - In secure locations	
Data Disposal	Does the agency have policies and procedures to dispose of hard copy PII or electronic media?	_____Y_____N - Agency shreds all hardcopy PII before disposal	
		Before disposal, the Agency reformats/degausses (demagnetizes):	
		_____Y_____N - Discs	
		_____Y_____N - CDs	
		_____Y_____N - Computer hard-drives	
		_____Y_____N - Other media (tapes, flash drives, etc.)	

Software Security	Do all HMIS workstations have current operating system and internet browser security? (This includes non-HMIS computers if networked with HMIS computers.)	Operating System (OS) Version: _____	
		_____Y_____N - All OS updates are installed	
		_____Y_____N - Most recent version of Internet Browser(s) is installed	

We affirm and certify the above information is true and that this organization, \_\_\_\_\_, is in full compliance with all requirements listed as “CHO” (Covered Homeless Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the Cape and Islands CoC HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

CHO Security Officer Name (Print): \_\_\_\_\_

CHO Security Officer Signature: \_\_\_\_\_

Date: \_\_\_\_\_

CHO Agency Administrator Name (Print): \_\_\_\_\_

CHO Agency Administrator Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## APPENDIX 10: WELLSKY DISASTER RECOVERY PLAN



# Information Technology Disaster Recovery Plan (ITDRP) 2021

**Iron Mountain Data Center**  
615 N 48<sup>th</sup> St  
Phoenix, Arizona 85008

**TierPoint Data Center**  
1764A Old Meadow Lane  
McLean, Virginia 22102

**WellSky Corporate Headquarters**  
11300 Switzer Rd  
Overland Park, KS 66210

System Categorization: **Moderate**


Software and services for realizing care's potential

## Table of Contents

Controlled Document Labeling.....	4
Approvals .....	4
Revision History.....	4
Statement of Authorization.....	4
Statement of Compliance Expectations.....	5
Statement of Purpose .....	5
Distribution Warning.....	5
Introduction.....	5
Background.....	6
Scope.....	7
Out of Scope .....	7
Assumptions .....	7
Concept of Operations .....	7
System Description .....	9
Diagram.....	9
Alternate Processing Site .....	10
Diagram.....	11
Essential Functions.....	11
Disaster Recover Team (DRT).....	11
DRT Roles and Responsibilities .....	12
Activation and Notification .....	13
Activation Criteria and Procedure.....	13
Notification .....	13
Outage Assessment.....	14
Outage Assessment.....	14
Prioritization .....	14
Impact Assessment (Functional).....	15
Impact Assessment (Information).....	15
Recoverability Effort Categories .....	15
Recoverability .....	15
Sequence of Recovery.....	16
Recovery Procedures.....	16
Recovery Escalation Notices/Awareness .....	16

<b>Reconstitution.....</b>	<b>17</b>
Validation Data Testing.....	17
Validation Functionality Testing .....	17
Recovery Declaration.....	17
Notification (Users) .....	17
Cleanup .....	17
Offsite Data Storage .....	17
Data Backup .....	18
Documentation.....	18
Deactivation .....	18
<b>Appendix A: Disaster Recovery Team Contact List .....</b>	<b>19</b>
Appendix A.1: ITDRP Organizational Chart .....	20

## Controlled Document Labeling

	<b>Information Technology Disaster Recovery Plan (ITDRP)</b>	
WellSky™ Corporation	Applicability: TierPoint Lenexa KS, Data Center Iron Mountain, PH Data Center	Document Number: <b>QMS 10.9a</b>

## Approvals

Chief Operating Officer S. Morgan Signature on File	Date 11/11/2021	Chief Technology Officer Joel Dolisey Signature on File	Date 11/11/2021
---	--------------------	---	--------------------

## Revision History

Version	Summary of Changes	Author	Date
1	Deactivation and revision of prior WellSky Corporation ITDRP. Incorporated all versions 1 through 16 into this new WellSky managed document. This document incorporates WellSky organizational changes.	J. Moeckel	11/07/2021

## Statement of Authorization

WellSky must develop, adopt, and adhere to a formal, documented contingency planning procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance. The appropriate level of information technology business continuity management must be in place to sustain the operation of critical information technology services to support the continuity of vital business functions and the timely delivery of critical automated business services to Clients.

Appropriate planning and testing processes must be in place to ensure that, in the event of a significant business interruption, critical production environments can be recovered and sustained to meet business requirements. To facilitate the effectiveness of systems and compliance with policy, coordination is required between WellSky Information Technology, Cloud Services, Development Operations, Information Security, Compliance, and Corporate Communications.

As the content authority for WellSky Corporation, TierPoint Lenexa, KS, Data Center (CORP-TierPoint) and Iron Mountain, PH, Data Center, I hereby certify that the information system disaster recovery plan (ITDRP) is complete, and that the information contained within the ITDRP provides an accurate representation of the application, its hardware, software, and telecommunication components.



I further certify that this document identifies the criticality of the system as it relates to the mission of WellSky, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

This document will be modified as changes occur and will remain under version control, in accordance with WellSky's contingency planning policy.

Authorization				
Authority	Name	Title	Signature	Date
Content	Collin Chan	Sr. VP, Engineering	Signature on File	11/07/2021
Approval	Jon Moeckel	Regulatory Compliance Manager	Signature on File	11/07/2021

### Statement of Compliance Expectations

Compliance with this plan is expected immediately. All recipients of this plan must ensure that their relevant procedures / plans are up to date and consistent with the contents of this overall plan. If there are any inconsistencies, please inform Collin Chan the Business Continuity Coordinator immediately.

### Statement of Purpose

The WellSky Information Technology Disaster Recovery Plan (ITDRP), SaaS Disaster Recovery Plans (SDRP) describes the response structure and outlines the accountabilities and interactions between internal functions and external agencies that may be called upon to ensure effective business recovery of critical processes.

### Distribution Warning

This document is the sole confidential property of WellSky Corporation (hereafter, WellSky) and may not be reproduced, in whole or in part, by any means without the prior written permission from the Coordinator of Business Continuity. A copy of the **Iron Mountain** Information Technology Disaster Recovery Plan will be distributed only after the Business Continuity Coordinator has secured the execution of a Non-Disclosure Agreement (NDA). All copies must be kept in a secure place. The Business Continuity Coordinator shall know of all such places and will be notified immediately if any of these documents are lost.

The information in this document is to be used for official purposes only.

### Introduction

Information systems are vital to WellSky's mission/business processes; therefore, it is critical that services provided by **Iron Mountain** are able to operate effectively without excessive interruption. This Information System Disaster Recovery Plan (ITDRP) establishes comprehensive procedures to recover **Iron Mountain** quickly and effectively following a service disruption.

## Background

This WellSky ITDRP has been developed to assure processes and procedures that support the restoration of the Information Technology (IT) infrastructure that supports products and services provided by WellSky Corporation at the Iron Mountain, Phoenix AX, Data Center. The recovery objectives of the IT infrastructure would be managed, as follows.

- Maximize the effectiveness of disaster/contingency operations through an established plan that consists of the following five (5) phases:
  - **Activation and Notification** – Activation of the ITDRP occurs after a disruption or outage that may extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss. Assembling the appropriate personnel at hand and deciding on a disaster declaration occurs within eight (8) hours of the original incident.
  - **Respond** - If a disaster is declared, this stage involves deployment of proper internal resources (staff) and external resources (vendors). System owners and users are notified of a possible long-term outage, and a thorough assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.
  - **Recovery** – The Recovery phase details the activities and procedures to restore CORP-TierPoint. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. The execution of the appropriate recovery procedures for the incident are based on information gathered during the assessment process and on conclusions reached during the response process.<sup>1</sup> This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.
  - **Reconstitution Phase** – The Reconstitution phase defines the actions taken to restore the system to normal business operations in the restored facility or new location. This includes execution of appropriate testing to ensure CORP-TierPoint is validated and that normal operations are resumed.
  - **Plan Deactivation** – Once all activities have been completed and documentation has been updated the Business Continuity Coordinator will deactivate the plan and provide notification to Executive Management and WellSky personnel. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

---

<sup>1</sup> If a disaster is declared, recovery requires restoration of critical/essential functionality within a maximum of forty-eight (48) hours from the time of the incident.



## Scope

This ITDRP has been developed for **Iron Mountain**, which is classified as a **Moderate** impact system. Procedures in this ITDRP are designed to recover **Iron Mountain** as follows:

Recovery Time/Point/Capacity Objectives	Target
RPO	One (1) Hour
RCO/RT0	Eight (8) Hours

This plan does not address replacement or purchase of new equipment, short term disruptions; or loss of data at the onsite facility or at the user-desktop levels. As **Iron Mountain** is a **Moderate** impact system alternate data storage and alternate site processing are not required.

The Scope of this recovery effort includes the following instance of recovery involving:

- The facilities and technology infrastructure that supports the products, operations, and services provided by WellSky Corporation at **Iron Mountain; Phoenix AZ** are included. In this instance of recovery, the WellSky World Headquarters office located in **Overland Park, Kansas**, and the computers and environments at the **TierPoint KS Data Center** would be unaffected.
- This includes all infrastructure required to support all development environments and associated business application infrastructure.

## Out of Scope

The scope of the recovery effort does not include:

- The IT equipment and applications housed at the **TierPoint Data Center** in **Lenexa, KS**.

## Assumptions

The following assumptions were used when developing this ITDRP:

- **Iron Mountain** has been established as a **Moderate** impact system.
- Alternate processing sites and offsite storage are required for this system.
- The **Iron Mountain** system is inoperable and cannot be recovered within eight (8) hours.
- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the **Iron Mountain ITDRP**.

The **Iron Mountain ITDRP** does not apply to the following situations:

- Emergency evacuation of personnel.
- Pandemic response plan.

## Concept of Operations

The Concept of Operations section provides details about **Iron Mountain**, an overview of the phases of the ITDRP (Activation and Notification, Recovery, and

Reconstitution), and a description of roles and responsibilities of WellSky's personnel during ITDRP activation.

Prevention is always the primary concern of any viable Information Technology & Business Resumption Planning program. However, an effective recovery plan balances strong preventative measures with clearly defined goals and supporting procedures that outline the steps to be taken in the case of a disaster. The following goal have been established for The WellSky resumption program. Specifically:

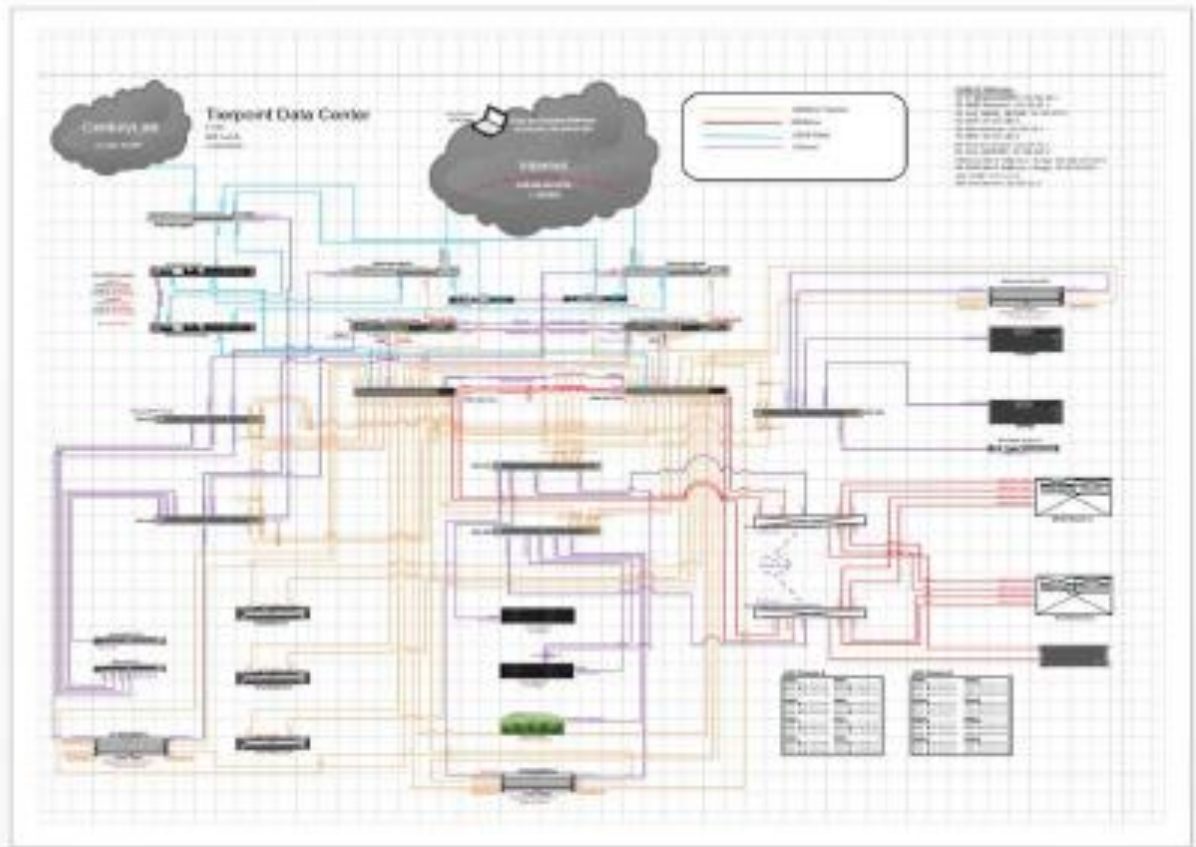
- To put into place preventative measures to reduce the possibility of an extended outage involving WellSky's operations, products, services, and SaaS infrastructure.
- Should a disaster occur, the goal is to minimize the amount of time required to recover operations, products, services, and SaaS infrastructure and data sing existing or replacement computer configurations.
- Restoration will be via re-purposing existing equipment at **TierPoint, Lenexa, KS** which is currently in operation and used as Development and COLO environment.
- The WellSky Resumption Plan developed for the recovery of **Iron Mountain** attempts to balance as much of the conflicting goals listed below as possible, specifically:
  - Simplicity in approach.
  - Completeness of recovery.
  - Minimize the effort on the operation of unplanned outages.
  - Speed of recovery.
  - Cost of recovery.
- The goal of this ITDRP is to provide adequate alternate computer system communications functionality, and office facilities in the event of a significant loss or site-specific disaster or disruption that affects the computing capability at **Iron Mountain**.
- The disaster recovery equipment is located in **TierPoint Data Center in Lenexa, KS**. This equipment will support:
  - 100% of the Business-Critical and essential production load for all operations and development systems at **Iron Mountain**.
  - 100% of the infrastructure computing capacity for all operational systems at **Iron Mountain**.
  - 100% of development storage capacity for all development environments.
  - No system production activity other that what is deemed to be essential (e.g., legislated changes)
- In the event of regional issues affecting the **Iron Mountain** data center location, alternate work locations for **WellSky** staff would be:
  - Remote at home.
  - For those that must travel to initiate a recovery at **TierPoint, Kansas** from the **WellSky World Headquarters** facility in **Overland Park, KS**.

#### System Description

<b>System Identifier</b>	
<b>Official System Name:</b>	WellSky Corporation,
<b>System Acronym:</b>	CORP
<b>Operational Status:</b>	<input checked="" type="checkbox"/> Operational <input type="checkbox"/> Under Development <input type="checkbox"/> Major Modification
<b>System Type:</b>	<input type="checkbox"/> Major Application (MA) <input checked="" type="checkbox"/> General Support System (GSS)

<b>System Identifier</b>	
<b>Official System Name:</b>	Iron Mountain, Phoenix AZ
<b>System Acronym:</b>	TierPoint
<b>Operational Status:</b>	<input checked="" type="checkbox"/> Operational <input type="checkbox"/> Under Development <input type="checkbox"/> Major Modification
<b>System Type:</b>	<input checked="" type="checkbox"/> Major Application (MA) <input checked="" type="checkbox"/> General Support System (GSS)

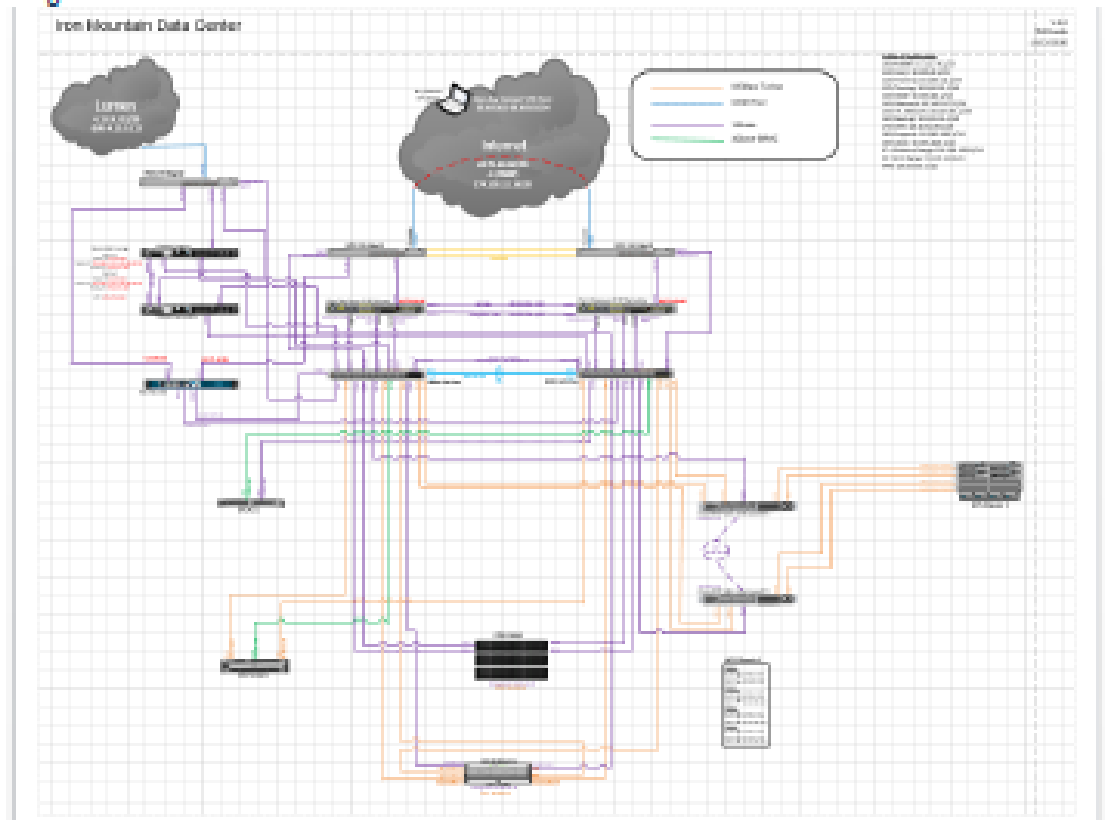
#### Diagram



#### Alternate Processing Site

System Identifier	
Official System Name:	TierPoint, Lenexa, KS
System Acronym:	Iron Mountain
Operational Status:	<input checked="" type="checkbox"/> Operational <input type="checkbox"/> Under Development <input type="checkbox"/> Major Modification
System Type:	<input checked="" type="checkbox"/> Major Application (MA) <input checked="" type="checkbox"/> General Support System (GSS)

## Diagram



## Essential Functions

Name	Contact	Phone	Email	Brief description of service or function
Engineering	Joel Dolley	512-965-9422	<a href="mailto:Joel.Dolley@wellsky.com">Joel.Dolley@wellsky.com</a>	CTO - Responsible for all Applications and Technology at WellSky
Operations	Steve Morgan	816-388-6889	<a href="mailto:Steve.Morgan@wellsky.com">Steve.Morgan@wellsky.com</a>	COO - Responsible for Operational Decisions at WellSky
People and Talent	Dana Streck	913-387-1080	<a href="mailto:Dana.streck@wellsky.com">Dana.streck@wellsky.com</a>	Sr. VP Responsible for People and Talent at WellSky
Legal	Rob Weber	608-347-5775	<a href="mailto:Rob.weber@wellsky.com">Rob.weber@wellsky.com</a>	CLO - Responsible for corporate counsel at WellSky
Client Services	Michael James	913-387-1031	<a href="mailto:Michael.james@wellsky.com">Michael.james@wellsky.com</a>	VP - Responsible for professional services at WellSky
Client Experience	John Hutchinson	913-387-1180	<a href="mailto:John.hutchinson@wellsky.com">John.hutchinson@wellsky.com</a>	Sr. VP - Responsible for customer support at WellSky
Solutions Management	Amy Shellhart	913-387-1159	<a href="mailto:Amy.shellhart@wellsky.com">Amy.shellhart@wellsky.com</a>	Sr. VP Product Management
Financial Services	Timothy Ashe	413-584-5300	<a href="mailto:Timothy.ashe@wellsky.com">Timothy.ashe@wellsky.com</a>	COO - WellSky Financial Services

## Disaster Recover Team (DRT)

The ITDRP establishes several roles for Iron Mountain recovery and reconstitution support. Persons or teams assigned ITDRP roles have been trained to respond to

disaster events affecting Iron Mountain. The DRT contact list is located in Appendix A.

#### DRT Roles and Responsibilities

Role	Responsibilities
Executive Management	Executive Management are not heavily involved with DR planning. They provide oversight and aid in the following: <ul style="list-style-type: none"> <li>• Strategy.</li> <li>• Policy</li> <li>• Budget</li> <li>• Dealing with</li> </ul>
Corporate Communications	Corporate Communications facilitates communications related to the event in a controlled and precise manner. Corporate Communications will provide: <ul style="list-style-type: none"> <li>• Internal communications, as needed.</li> <li>• Client communications, as needed.</li> <li>• External communications (i.e., media, corporate partners), as needed.</li> </ul>
Corporate Counsel	Corporate Counsel coordinates all legal activities related to the disaster event. <ul style="list-style-type: none"> <li>• Prepare and executes WellSky standard agreements with identified partners or service providers.</li> <li>• Reviews and reports contractual requirements of affected Clients.</li> <li>• Collaborates with Corporate Communications to create FAQ and control messaging.</li> </ul>
Regulatory Compliance	The Regulatory Compliance Manager monitors the contingency plan and aids the Contingency Coordinator in coordinating the contingency plan, training and awareness, exercises, and testing.
Contingency Coordinator/Manager	<ul style="list-style-type: none"> <li>• Activate WellSky's applicable Contingency Plan.</li> <li>• Activate WellSky's applicable Reconstitution Plan.</li> <li>• Review and approve event specific reconstitution POA(s).</li> <li>• Active teams at an alternate location to ensure contingency of essential functions.</li> <li>• Account for organizational personnel.</li> </ul>
Reconstitution Manager(s)	<ul style="list-style-type: none"> <li>• Assemble the Reconstitution Planning Team at a safe location.</li> <li>• Manage development of event-specific reconstitution POA(s).</li> <li>• Identify appropriate SMEs (Reconstitution Implementation Team members), partners, and service provider to respond to the specific event.</li> <li>• Coordinate for the implementation of agreements with partners and service providers.</li> </ul>

	<ul style="list-style-type: none"> <li>• Coordinate leadership approval of reconstitution POA(s).</li> </ul>
Reconstitution Team Member(s)	<ul style="list-style-type: none"> <li>• Report to identified/designated locations.</li> <li>• Conduct/arrange for preliminary damage assessment using the building assessment checklist.</li> <li>• Reach consensus regarding the appropriate planning level.</li> <li>• Tailor WellSky's Reconstitution Plan to conform to the specific event.</li> <li>• Develop event specific POA(s).</li> <li>• Prepare to transition from planning to implementation on Leadership order to implement.</li> </ul>

### Activation and Notification

The Activation and Notification Phase defines initial actions taken once Iron Mountain disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ITDRP. At the completion of the Activation and Notification Phase, Iron Mountain DRT will be prepared to perform recovery measures to restore system functions.

#### Activation Criteria and Procedure

The Iron Mountain ITDRP may be activated if one or more of the following criteria are met:

- The type of outage indicates CORP-TierPoint will be down for more than eight (8) hours.
- The facility housing CORP-TierPoint is damaged and may not be available within eight (8) hours.

The Business Continuity Manager or Executive Management may activate the ITDRP if one or more of these criteria are met.

#### Notification

The first step upon activation of the Iron Mountain ITDRP is notification of appropriate business and system support personnel. Contact information for appropriate POCs is included in Appendix A.

WellSky controls ITDRP communications for all internal and external stakeholders. Internal messaging and risk communications during contingency event will be conducted by the Business Continuity Coordinator. External messaging and risk communication during contingency event will be conducted by VP of Communications. Process on alert and notification will be determined based off of identified threat and impact. The VP of Communications will establish and implement the necessary communications.



## Outage Assessment

WellSky will determine how the ITDRP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment is completed as quickly as possible. WellSky's outage assessment procedures are unique for the particular system, but the following minimum areas are addressed:

- Cause of the outage or disruption.
- Potential for additional disruption or damage.
- Status of physical infrastructure (i.e., structural integrity of computer room, condition of electric power, telecommunications, and HVAC).
- Inventory and functional status of system equipment (i.e., fully functional, partially functional, nonfunctional).
- Type of damage to system equipment or data (i.e., water, fire and heat, physical impact, electrical surge).
- Items to be replaced (i.e., hardware, software, firmware, supporting material).
- Estimated time to restore normal services.

## Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by the DRT. Assessment results are provided to the Business Continuity Coordinator to assist in the coordination of the recovery of Iron Mountain

The DRT will work quickly to analyze and validate the outage, following a pre-defined process and documenting each action taken. When an outage has occurred, the DRT will rapidly perform an outage assessment to determine the scope, such as:

- Which systems, networks, applications, and data were affected?
- Origination of the outage.
- How the occurred occurring (i.e., attack methods being used, vulnerabilities being exploited, etc.).

## Prioritization

WellSky does not manage outages on a first come, first serve basis. Instead, handling is prioritized based on the following relevant factors:

- **Functional Impact of the Outage** – Outages involving IT systems typically impact business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. The DRT considers how the outage impacts the current and future functionality of the affected systems.
- **Information Impact of the Outage** – Outages may affect the confidentiality, integrity, and availability of information. The DRT considers how this information exfiltration will impact the overall mission of WellSky and clients.
- **Recoverability from the Outage** – The extent of the outage and the type of resources it affects determine the amount of time and resources that must be spent on recovery. The DRT considers the effort necessary to actually recover



from the outage and carefully weighs that against the value the recovery effort will create, and any requirements related to outage.

Combining the functional impact and the impact to the information determines the business impact of the outage. The recoverability of the outage determines the possible responses that the DRT may take when handling the outage.

#### Impact Assessment (Functional)

Category	Description
None	No effect to WellSky's ability to provide all services to all users.
Low	Minimal effect: the organization can still provide critical services to all users but has lost efficiency.
Medium	WellSky has lost the ability to provide a critical service to a subset of system users.
High	WellSky is no longer able to provide some critical services to any users.

#### Impact Assessment (Information)

Category	Description
None	No information was exfiltrated, changed, deleted, or otherwise compromised.
Privacy Incident	Sensitive personally identifiable information (PII), protected health information (PHI), or payment card information (PCI) was accessed or exfiltrated.
Proprietary Incident	Classified (internal/restricted/confidential) proprietary information was accessed or exfiltrated.
Integrity Loss	Sensitive or proprietary information was changed or deleted.

#### Recoverability Effort Categories

Category	Description
Regular	Time to recovery is predictable with existing resources.
Supplemented	Time to recovery is predictable with additional resources.
Extended	Time to recovery is unpredictable: additional resources and outside help are needed.
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly), launch investigation.

### Recoverability

The Recovery Phase provides formal recovery operations that begin after the ITDRP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, Iron Mountain will be functional and capable of performing the functions identified in the system description.

### Sequence of Recovery

Recovery procedures will reflect system priorities identified in the ITDRP. The sequence of activities will avoid significant impacts to related systems. Procedures will be written in a stepwise, sequential format so system components are restored in a logical manner. The procedures will include escalation steps and instructions to coordinate with other teams when certain situations occur, such as:

- An action is not completed within the expected period.
- A key step has been completed.
- Item(s) must be procured.
- Other system-specific concerns exist.

The following activities occur during recovery of Iron Mountain.

- Identify recovery location (if not at original location).
- Identify resources to perform recovery procedures.
- Retrieve backup and system installation media.
- Recover hardware and operating system (if required).
- Recover system from backup and system installation media.

### Recovery Procedures

The following procedures are provided for recovery of Iron Mountain at the original or established alternate location. Recovery procedures are outlined per team and should be expected in the sequence presented to maintain an efficient recovery effort.

The ITDRP Recovery Procedures provide detailed procedures to restore the information systems or components to a known state. Procedures will be assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic areas.
- Notifying internal and external business partners associated with the system.
- Obtaining necessary office supplies and workspaces.
- Obtaining and installing necessary hardware components.
- Obtaining and loading backup media.
- Restoring system data to a known state.
- Restoring critical operating system and application software.
- Testing system functionality including security controls.
- Connecting system to network or other external systems.
- Operating alternate equipment successfully.

### Recovery Escalation Notices/Awareness

Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. The Business Continuity Coordinator will conduct internal messaging. External messaging and communication during recovery will be conducted by the VP of Communications. Specific processes will be developed in real time, commensurate with the impact of the event. The VP of Communications will establish and implement the necessary communications.

## Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone notable change and will require assessment and reauthorization. The phase consists of two major activities:

- Validating successful reconstitution.
- Deactivation of the plan.

### Validation Data Testing

Validation data testing is the process of testing and validating data to ensure that data files or databases have been removed completely at the permanent location. The following procedures will be used to determine that the data is complete and current to the last available backup.

### Validation Functionality Testing

Validation functionality testing is the process of verifying that recovered Iron Mountain functionality has been evaluated, and the system is ready to return to normal operations.

### Recovery Declaration

Upon successfully completing testing and validation, the Business Continuity Coordinator will formally declare recovery efforts complete, and that CORP-TierPoint is in normal operations. Iron Mountain Business and technical POCs will be notified of the declaration by the Business Continuity Coordinator.

### Notification (Users)

Upon return to normal system operations Iron Mountain clients will be notified by VP, Communications using predetermined notification methods (i.e., email, phone call, town hall, etc.).

### Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manual or other documentation to their original locations, and readying the system for possible a future contingency event.

### Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

#### Data Backup

As soon as reasonable following recovery, the system will be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are.

#### Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ITDRP. It is the responsibility of each Reconstitution Team to document their actions during the recovery and reconstitution effort and provide that documentation to the Regulatory Compliance Manager. Types of documentation that should be generated and collected after plan activation include, but are not limited to:

- Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities).
- Functionality and data testing results.
- Lessons learned documentation (After Action Review).

#### Deactivation

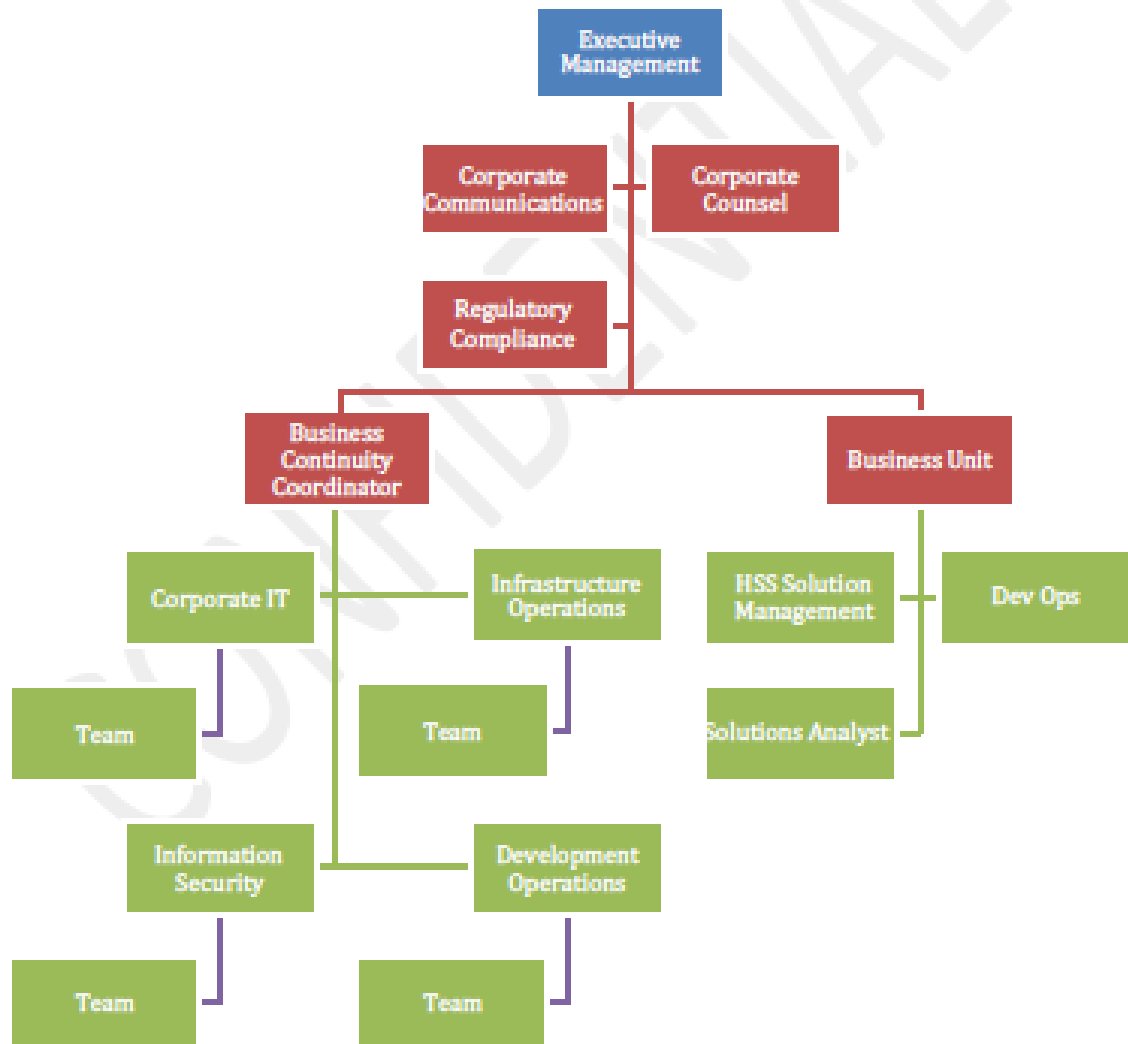
Once all activities have been completed and documentation has been updated, the Business Continuity Coordinator will formally deactivate the ITDRP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

## Appendix A: Disaster Recovery Team Contact List

Name	Department/Business Unit	Primary Contact	Alternate Contact
Business Continuity Coordinator	Sr. VP Engineering	Name: Collin Chan E-Mail: <a href="mailto:collin.chan@wellsky.com">collin.chan@wellsky.com</a> Telephone: Cell Phone:	Name: E-Mail: Telephone: Cell Phone:
Corporate Communications	VP, Communications	Name: Amy Kaminski E-Mail: <a href="mailto:Amy.kaminski@wellsky.com">Amy.kaminski@wellsky.com</a> Telephone: 913-307-1083 Cell Phone: 816-582-4490	Name: Shoma Thomas E-Mail: <a href="mailto:shoma.thomas@wellsky.com">shoma.thomas@wellsky.com</a> Telephone: Cell Phone:
Legal	Corporate Counsel	Name: Sarah Rapelye E-Mail: <a href="mailto:sarah.rapelye@wellsky.com">sarah.rapelye@wellsky.com</a> Telephone: 913-307-1114 Cell Phone: 816-679-4208	Name: E-Mail: Telephone: Cell Phone:
Regulatory Compliance	Regulatory Compliance Manager	Name: Jon Moeckel E-Mail: <a href="mailto:jon.moeckel@wellsky.com">jon.moeckel@wellsky.com</a> Telephone: 913-307-1051 Cell Phone: 913-952-2031	Name: E-Mail: Telephone: Cell Phone:
Reconstitution Manager (Information Security)	Sr. Director Engineering (Information Security)	Name: Jami Albre-Fisher E-Mail: <a href="mailto:jami.albre-fisher@wellsky.com">jami.albre-fisher@wellsky.com</a> Telephone: 413-584-5300 Cell Phone: 413-386-5909	Name: E-Mail: Telephone: Cell Phone:
Reconstitution Manager (Corporate IT)	Director Engineering	Name: Jim Burkholder E-Mail: <a href="mailto:jim.burkholder@wellsky.com">jim.burkholder@wellsky.com</a> Telephone: 913-307-1021 Cell Phone: 913-653-1341	Name: Collin Chan E-Mail: <a href="mailto:collin.chan@wellsky.com">collin.chan@wellsky.com</a> Telephone: Cell Phone:
Reconstitution Manager (Infrastructure Operations)	Sr. Manager, Infrastructure Operations	Name: Andrew Blasman E-Mail: <a href="mailto:Andrew.blasman@wellsky.com">Andrew.blasman@wellsky.com</a> Telephone: 614-543-8801 Cell Phone: 330-437-8534	Name: E-Mail: Telephone: Cell Phone:
Reconstitution Manager HSS DevOps	Director, Engineering	Name: Tom Walton E-Mail: <a href="mailto:tom.walton@wellsky.com">tom.walton@wellsky.com</a> Telephone: 913.307.1164 Cell Phone:	Name: Scott Lloyd E-Mail: <a href="mailto:Scott.Lloyd@wellsky.com">Scott.Lloyd@wellsky.com</a> Telephone: Cell Phone:
Reconstitution Team HSS DevOps	Manager, Engineering	Name: Anurag Acharya E-Mail: <a href="mailto:anurag.acharya@wellsky.com">anurag.acharya@wellsky.com</a> Telephone: Cell Phone:	Name: Tom Walton E-Mail: <a href="mailto:tom.walton@wellsky.com">tom.walton@wellsky.com</a> Telephone: 480.831.7800xt 14040 Cell Phone:
Reconstitution Team HSS DevOps	Staff Software Engineer	Name: Tola Akingbo E-Mail: <a href="mailto:tola.akingbo@wellsky.com">tola.akingbo@wellsky.com</a> Telephone: 703.657.1522xt 15522 Cell Phone:	Name: E-Mail: Telephone: Cell Phone:
Reconstitution Team HSS DevOps	Staff Software Engineer	Name: Jack Bove E-Mail: <a href="mailto:jack.bove@wellsky.com">jack.bove@wellsky.com</a> Telephone: 703.657.1482 Cell Phone:	Name: Betsy Classen E-Mail: <a href="mailto:betsy.classen@wellsky.com">betsy.classen@wellsky.com</a> Telephone: Cell Phone:
Reconstitution Manager HSS Infrastructure	Manager, Engineering	Name: Shahid Hameed E-Mail: <a href="mailto:shahid.hameed@wellsky.com">shahid.hameed@wellsky.com</a>	Name: E-Mail:

		Telephone: 703.657.1450 Cell Phone:	Telephone: Cell Phone:
Reconstitution Team HSS Infrastructure	Sr. System Engineer	Name: Will Lamb E-Mail: <a href="mailto:will.lamb@wellsky.com">will.lamb@wellsky.com</a> Telephone: 913.307.1046 Cell Phone:	Name: E-Mail: Telephone: Cell Phone:
Reconstitution Team HSS Infrastructure	Systems Engineer	Name: Allen Knowles E-Mail: <a href="mailto:allen.knowles@wellsky.com">allen.knowles@wellsky.com</a> Telephone: 913.307.1123 Cell Phone:	Name: E-Mail: Telephone: Cell Phone:

Appendix A.1: ITDRP Organizational Chart



## APPENDIX 11: DATA COLLECTION NOTICE

### Data Collection Notice

---

We collect personal information directly from you for reasons that are discussed in our privacy statement.

We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons.

We only collect information that we consider to be appropriate.

### Recopilación de Datos

---

Recopilamos información personal directamente de usted por las razones que se discuten en nuestra declaración de privacidad.

Podemos ser requeridos recopilar alguna información personal por ley o por las organizaciones que nos dan dinero para operar este programa. Otra información personal que recopilamos es importante para ejecutar nuestros programas, mejorar los servicios para las personas sin hogar, y para comprender mejor las necesidades de las personas sin hogar.

Nosotros solamente recopilamos información que consideramos apropiado.

## APPENDIX 12: PRIVACY NOTICE – ENGLISH



### Cape Cod and Islands CoC HMIS Privacy Notice

This notice describes how we may use and share information we have about you and how you can access that information.

HMIS is a database that stores information about clients we serve and services we provide. We collect information that is defined in the U.S. Department of Housing and Urban Development's HMIS Data Standards. This notice applies to the Cape Cod and Islands CoC HMIS system.

#### Uses and Disclosures of Your Information

Information you provide:

- Will be entered into the Cape Cod and Islands CoC HMIS database known as ETO.
- Will be used to improve, provide, and coordinate services.
- May be used in relation to payment or reimbursement for services.
- Will be used to make sure that our programs are effective.
- Will be used to prepare statistical reports, but only aggregate data will be provided to funders, media, or any state or local agency. No social security numbers, Date of birth or names will be released without your written consent and consent between the sender and receiver of the information. You may revoke this consent at any time.

Information you provide about physical or mental health problems will not be shared with other service providers unless you have authorized it.

Personally Identifiable Information (PII) will be shared only if you authorize it or if required by law, or if there is a serious threat to health or safety.

In Massachusetts, PII includes your name, date of birth, social security number, driver's license number, and bank account numbers. We **DO NOT** collect driver's license or bank account numbers.

#### Your Rights

- Your right to receive services will not be affected if you refuse to provide HMIS information.



- You control who your information is shared with. You may allow or refuse to share your information with other service providers.
- You may give written notice to end all privacy and information sharing agreements at any time.
- You may have a copy of this notice.
- You may view your record, have your record corrected, and file a complaint.

## How to Inspect and Correct Your Personal Information

You may request a copy of your HMIS record. Please submit a verbal or written request to program staff to get a copy. We will explain any information on it that you do not understand.

We will consider your request to correct inaccurate or incomplete personal information. We may delete or fix information that we agree is inaccurate or incomplete.

We may deny your request to inspect your personal information if:

- The information was gathered in reasonable anticipation of legal actions.
- The information would violate a confidentiality agreement.
- Sharing the information would endanger the life or safety of any individual.

If we deny your request, we will explain the reason. We will keep a record of the request and the reason it was denied.

## Data Storage and Disposal

We dispose of personal information that is not being used **seven (7)** years after it was created or updated. We may remove personal identifiers from the information instead of getting rid of it. We may keep information longer if required by laws, statutes, regulations, or contracts.

For more information contact the supervisor of your program.

To file a complaint, contact the Cape Cod and Islands HMIS System Administrator:

Martha Taylor  
Barnstable County Department of Human Services  
P.O. Box 427  
Barnstable, MA 02630  
(508) 375-6625  
[martha.taylor@barnstablecounty.org](mailto:martha.taylor@barnstablecounty.org)

*We have the right to change this notice at any time and changes may apply to information collected prior to the date of the change.*

*We accept and consider all questions or complaints regarding the Cape Cod and Islands Continuum of Care HMIS.*

## APPENDIX 13: PRIVACY NOTICE - SPANISH



### HMIS del Condado de Cape Cod and Islands Notificación de Privacidad

Este aviso describe como podemos utilizar y compartir la información que tenemos sobre usted y como usted puede tener acceso a esa información.

HMIS es una base de datos que almacena información acerca de los clientes que servimos y servicios que ofrecemos. Recopilamos la información que se define en el Departamento de Vivienda y Estándares de Datos HMIS de Desarrollo Urbano del EE. UU.. Este aviso se aplica al HMIS del Condado de Cape Cod and Islands.

#### Usos y Divulgaciones de su información

La información que usted proporcione:

- Se introducirá en el HMIS del Condado de Cape Cod and Islands.
- Se utilizará para mejorar, proveer y coordinar servicios.
- Puede ser utilizado en relación con el pago o reembolso de los servicios.
- Se utilizará para asegurar que nuestros programas sean eficaces.
- Se utilizará para preparar informes estadísticos.

La información que usted proporciona acerca de problemas de salud física o mental no será compartida con otros proveedores de servicios, a menos que usted haya autorizado.

Información de identificación protegida (PII) será compartida solo si usted lo autorice, o si lo requiere la ley, o si hay una amenaza seria a la salud o la seguridad.

En Massachusetts, PII incluye su nombre, fecha de nacimiento, número de seguro social, número de licencia de conducir y números de cuentas bancarias. No recopilamos números de licencia de conducir o cuentas bancarias.

#### Sus Derechos

- Su derecho a recibir los servicios no se verá afectado si se niega a proporcionar información de HMIS.
- Usted controla con quien su información se comparte. Puede permitir o denegar compartir su información con otros proveedores de servicios.
- Puede dar aviso por escrito para terminar los acuerdos del intercambio de información y privacidad en cualquier momento.
- Puedes obtener una copia de este aviso.
- Usted puede ver su expediente, tener su expediente corregido, y someter una queja.

## Como revisar y corregir su información personal

Usted puede solicitar una copia de su expediente HMIS. Por favor, envíe una solicitud verbal o por escrito al personal del programa para obtener una copia. Explicaremos cualquiera información que no entiende.

Consideraremos su solicitud para corregir la información personal que este inexacta o incompleta. Podemos eliminar o corregir la información en que estemos de acuerdo ser inexacta o incompleta.

Podemos negar su solicitud para revisar su información personal si:

- La información se recopilo en anticipación razonable de acciones legales.
- La información violaría un acuerdo de confidencialidad.
- Compartir la información pondría en peligro la vida o seguridad de cualquier persona.

Si negamos su petición le explicaremos la razón. Vamos a mantener un registro de la solicitud y la razón por la que fue denegada.

## Almacenamiento de Datos y Eliminación

Disponemos información personal que no esta siendo utilizado **siete (7) años** después de su creación o actualización. Podemos quitar los identificadores personales de la información en lugar de deshacerse de ella.

Podemos mantener la información por más tiempo si lo requieren las leyes, estatutos, reglamentos o contratos.

-----  
Para mas información póngase en contacto con el supervisor de su programa.

Para someter una queja, comuníquese con la administrador del sistema del HMIS.

Martha Taylor  
Barnstable County Department of Human Services  
P.O. Box 427  
Barnstable, MA 02630  
(508) 375-6625  
[martha.taylor@barnstablecounty.org](mailto:martha.taylor@barnstablecounty.org)

*We have the right to change this notice at any time and changes may apply to information collected prior to the date of the change.*

*We accept and consider all questions or complaints regarding the Cape Cod and Islands Continuum of Care HMIS.*

## APPENDIX 14: AUTHORIZATION FOR RELEASE OF PROTECTED INFORMATION



### MA-503 CAPE COD AND ISLANDS CoC HOMELESS MANAGEMENT INFORMATION SYSTEM AUTHORIZATION FOR RELEASE OF PROTECTED INFORMATION

When \_\_\_\_\_ (print name of Interviewer's Organization) collects certain information about you, that information is protected under state and federal legal requirements. Information that includes references to substance use, a diagnosis of substance use disorder, or treatment for substance use disorder; diagnosis, treatment, or referrals related to a mental health disorder or HIV/AIDS, including progress notes and psychotherapy notes; and domestic violence concerns may not be shared with other participating Agencies without your written consent, unless otherwise permitted or required by law.

I, \_\_\_\_\_ (print name of Participant), have read and fully understand this authorization form, and I authorize the Interviewer's Organization, named above, to share my **protected information** with the member agencies of the Cape & Islands Regional Network on Homelessness (the Network) and the Cape Cod and Islands Continuum of Care (CoC), for the purpose of entering my data into the MA-503 Cape Cod and Islands Continuum of Care Homeless Management Information System ("HMIS"). The Network is a collaborative of state, county and local government agencies, social service providers, housing agencies, businesses, law enforcement, and other organizations that serve homeless and formerly homeless persons in the Cape and Islands Region. The Continuum of Care (CoC) Grant Program is a homeless assistance program administered by the U.S. Department of Housing and Urban Development (HUD).

- I understand my **protected information** and records are safeguarded by federal, state, and local regulations. I understand my **protected information** cannot be shared without my written consent unless such disclosure is allowed by law.
- I understand that **protected information** collected about me in the interview process can be shared with the designated, authorized staff persons at the CoC HMIS and at organizations in the CoC identified on the attached list only to the extent that information is necessary for the referral process to housing and services appropriate for me, and that information will be: (i) my name and contact information, (ii) the optional name and contact information of another person, if provided below, who knows how to contact me, and (iii) the information I provide as part of the interview.
- I understand that my **protected information** can be shared only with organizations identified on the attached list. If the CoC wants to share my **protected information** with organizations not on the attached list, the CoC must first obtain my written consent to release the information unless otherwise authorized by law.
- I understand that I can ask for a complete list of Network members and participating HMIS agencies at any time by contacting the CoC at (508) 375-6625 or at [martha.taylor@barnstablecounty.org](mailto:martha.taylor@barnstablecounty.org).
- I understand that I may revoke this authorization to share my **protected information** at any time by notifying the HMIS System Administrator in writing:  
*Martha Taylor – Barnstable County Department of Human Services*  
*3195 Main Street – PO Box 427*  
*Barnstable, MA 02630*  
[martha.taylor@barnstablecounty.org](mailto:martha.taylor@barnstablecounty.org)
- I further understand if I revoke this authorization, the revocation will not apply to information that has already been used or disclosed.
- I understand that this authorization remains in effect during my participation in the CoC HMIS.
- I understand that, in any event, this authorization automatically expires 90 days after the completion of my participation in the CoC HMIS.
- I acknowledge that I have received a copy of this Authorization for Release of Protected Information.

Date \_\_\_\_\_ Signature (or mark) of Participant \_\_\_\_\_

Signature of Interviewer \_\_\_\_\_

Name of Alternate Contact \_\_\_\_\_ Contact Method \_\_\_\_\_