HMIS Policies and Procedures

Marla G. Simpson
Executive Director
Brooklyn Community Services
285 Schermerhorn Street
Brooklyn, NY 11217
(718) 310-5600
www.wearebcs.org

Table of Contents

1. BCS Communications

It is the policy of BCS that all internal communication practices for HMIS matters will be sent directly to the BCS HMIS Administrator. Individual BCS end users must communicate all HMIS Project or Data Warehouse matters to the BCS HMIS Administrator and all HMIS security matters to the BCS Security Contact, in addition to the BCS HMIS Administrator. BCS HMIS Administrator is responsible for communicating to all BCS end users any HMIS information that is relevant to the end user.

1.1. Technical Requirements

BCS is responsible for maintaining a project-level HMIS-compliant system for every project required to participate in HMIS and any other project voluntarily participating in HMIS.

1.1.1. Technical Standards for Project-level HMIS-compliant Systems

BCS uses Foothold AWARDS as a Data Warehouse system. It meets the following concerns:

- Recording client data from a limitless number of service transactions
- Preserving all required historical data to securing the data
- Collecting data on system use for the purposes of data quality and security, including login attempts, search parameters, and incidents of changes made to records.
- Collecting all program descriptor, universal, and program-specific data elements
- Meeting technical security requirements specified in Section 4 of these policies and procedures and technical privacy requirements specified in Section 6 of these policies and procedures

1.1.2. Data Upload Hardware/Software requirements

BCS uses Foothold AWARDS to upload data to HUD. It is the policy of BCS, to communicate any Data Warehouse issues to the HMIS Coordinator within 3 business days of the onset of the issues.

1.2. BCS End Users

BCS HMIS Administrators will provide user names and initial passwords to each Participating Agency user. User names will be unique for each user and will not be exchanged with other users.

BCS HMIS Administrators will provide unique user names and initial passwords to each user upon completion of training and signing of a confidentiality agreement and receipt of the Policies and Procedures Manual. The sharing of user names will be considered a breach of the HMIS Agency Agreement. BCS HMIS administrator will keep:

1. A list of usernames
2. Access authorization
3. User levels
4. Process for activating a user

1.2.1. BCS User Agreement

It is the policy of BCS that prior to being granted access to any project-level HMIS-compliant system, each new end user must sign an HMIS User Agreement indicating that he or she has received all required HMIS training and has read, understood and agrees to fulfill all of the obligations contained in these policies and procedures. Within six months of the effective date of these policies and procedures, all existing users must sign a User Agreement. An example of such a User Agreement is provided in Appendix G.

Each BCS HMIS Administrator will be responsible for the distribution, collection and storage of signed User Agreements. The signed HMIS User Agreements will be available for inspection at any time by the CCoC, through the HMIS Lead or Data Management Committee.

1.2.2. User Agreement Breach

It is the policy of BCS that a user who breaches the terms of the End User Agreement will face the sanctions specified by BCS. However, any breaches related to security or privacy will be reported to the HMIS Lead within 3 business days of discovery. These breaches will be dealt with on a case by case basis. Penalties may include, but are not limited to, temporary or permanent ban from using project-level HMIS-compliant system and legal action.

Breach of the User Agreement

It is the policy of BCS that the unauthorized use or disclosure of PII is considered a serious matter and will result in penalties or sanctions, which may include:

1. The loss of use or limitation on the use of the project-level HMIS-compliant system and other office and technology resources
2. Financial liability for the cost of such use
3. Adverse employment actions including dismissal
4. Civil and/or criminal prosecution and penalties.

1.3. Training Requirements

It is BCS policy that all end users are appropriately trained on system use, privacy, security, and data collection requirements. The HMIS Lead will provide training to BCS HMIS Administrators and Security Contacts to ensure they are adequately trained to provide such trainings to their end users. At the discretion of the HMIS Lead, additional trainings may be offered to BCS HMIS Administrators, Security Contacts, and other users.

BCS will develop and implement appropriate training for all end users on system use, privacy, security, and data collection requirements. To support this, the HMIS Lead will offer trainings and train-the-trainer sessions to all BCS HMIS Administrators and Security Contacts initially, prior to executing a Participation Agreement and annually or as needed to review updates, changes, or to refresh users. The HMIS Lead may conduct additional trainings at its discretion.

At minimum, the trainings offered by the HMIS Lead will cover:

- Train-the-trainer on HMIS Basics: Privacy, security and data collection requirements as set forth in these policies and procedures
- HMIS for Administrators: Managing data quality and project performance management using HMIS
- HMIS for Security Contacts: In-depth security training

BCS is responsible for training all end users on the use of its project-level HMIS-compliant system before the user is authorized to collect and enter data in the project-level HMIS-compliant system for upload to the Data Warehouse. From time to time, and at the discretion of the HMIS Lead, the HMIS Lead will provide training on the use of the AWARDS system for those BCS staff using AWARDS as their project-level HMIS compliant system.

BCS will indicate in the Administrative and Software Certification whether or not each end user has received appropriate training on system use, privacy, security, and data collection requirements consistent with the train-the-trainer sessions provided by the HMIS Lead and these policies and procedures.

1.4. Compliance

BCS is determined to communicate with the HMIS Lead frequently to ensure that requirements and obligations established in the Participation Agreement are being met.

2. HMIS Security Plan

BCS has HIPAA security policies and procedures.

2.1. HMIS Lead Security Officer and BCS Security Contact Roles and Responsibilities

BCS has designated a NYC HMIS Security Contact who is responsible for ensuring that BCS is meeting the minimum security requirements established in the Security Plan and the HMIS Participation Agreement, and is authorized by the Executive Director.

BCS has named the HMIS Lead Security Officer in the HMIS Lead Security Certification document, which will be updated at least annually. The contact information is incorporated into this Security Plan by reference. The duties of the Security Officer must be included in the individual's job description or HMIS Lead Security Certification, and signed by the Security Officer to indicate understanding and acceptance of these responsibilities. These duties include, but may not be limited to:

- Cooperatively with the HMIS Administrator, review the Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, work with the HMIS Administrator to develop recommendations to the Data Management Committee for review, modification, and approval.

- Annually review the HMIS Lead Security Certification document, test the HMIS Lead security practices for compliance, and work with the HMIS Administrator to coordinate communication with FTS to confirm security compliance of the Data Warehouse.

- Using the HMIS Lead Security Certification document, certify that the HMIS Lead adheres to the Security Plan or develop a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over as short a period of time as is possible.

- Implement any approved plan for mitigation of shortfalls and provide appropriate updates on progress to the Steering Committee.

- Respond, in cooperation with the HMIS Administrator, to any security questions, requests, or security breaches to the DHS System Administrator and Security Officer, and for communicating security-related HMIS information relayed from DHS to the organization's end users.

BCS will provide the name and contact information of the Security Contact at least annually in the Security Certification document. Changes to the individual named as the Security Contact that occur during the course of the year will be communicated via email to the HMIS Lead System Administrator and Security Officer within thirty days of the change.

The duties of the Security Contact must be included in the individual's job description or Security Certification document, and signed by the Security Contact to indicate understanding and acceptance of these responsibilities. These duties include, but may not be limited to:

- Annually review the Security Certification document, test the BCS security practices for compliance, and work with appropriate vendors (where applicable) to confirm security compliance of the project-level HMIS-compliant system.

- Using the Security Certification document, certify that the BCS adheres to the Security Plan or provide a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over time.

- Communicate any security questions, requests, or security breaches to the DHS System Administrator and Security Officer, and security-related HMIS information relayed from DHS to the BCS's end users.

- Complete security training offered by the HMIS Lead.

Additional duties that may be incorporated in the BCS Participation Agreement on a case-by-case basis include:

- Provide security training to the organization's end users based on Security training provided to the Security Contact by the HMIS Lead.

Any security-related questions from BCS staff will be communicated to DHS via the Security Contact, consistent with Section 2.3 of these policies and procedures.

2.2. Compliance Review

BCS will conduct a security review annually and certify that each participating project is in compliance with the NYC HMIS Security Plan and HUD standards.

BCS's Security Contact will be testing its security practices and completing the Security Certification document annually. This document is provided in Appendix E.

2.3. Criminal Background Verification

BCS staff in HMIS programs undergo criminal background verification. Record of the completed background check (though not the results) are available for inspection by the CoC.

BCS follows its own policies regarding conducting background checks and hiring individuals with criminal justice histories.

2.3.1. Annual Security Training

BCS requires a security training provided by the HMIS Lead prior to gaining system access to AWARDS and at least annually thereafter.

2.4. Data Warehouse Security

BCS uses AWARDS as the Data Warehouse. BCS End users of the Data Warehouse understand security-related requirements, are prohibited from sharing their username or password with any other individual, and are required to maintain the security and confidentiality of HMIS data in any format.

2.4.1. Boundary Protection

All BCS' computers, accessing AWARDS to upload data, are protected by a firewall.

2.4.2. System Access User Authentication and Passwords

All BCS users will be given a unique username and password to log into AWARDS. Default passwords must be changed upon the initial login. Passwords must be at least 8 characters and must contain at least one upper case letter, at least one lower case letter, and at least one alphanumeric character and at least one character which is numeric or a special character. Passwords must not be composed of easily guessed words, such as a user's own user ID, proper names (such as the user, application, or vendor name), or other criteria that can be associated to the user, or any of those spelled backwards. Users should not select passwords that contain personally identifiable numbers such as their phone extension, Social Security Number or home zip code. The system will automatically require each user to change his or her password at least every 90 days to a new password that is not the same as his or her previous four (4) passwords, and password cannot be changed more than once per day. Users shall not share their passwords. Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.

- AWARDS has been set up to provide the following safeguards against access by unauthorized users:

- Requires users to log in
- Users will not be allowed to log into AWARDS from multiple locations simultaneously.
- AWARDS users will be automatically logged off of the system after 20 minutes of inactivity.
  The user will be required to re-enter their username and password to regain access to the system.
- In the event that an AWARDS user forgets his or her password, users cannot retrieve forgotten passwords as they are not stored in the system but must instead create a new password with the assistance of the System Administrator or HMIS Coordinator. Users can change passwords on their own.

2.4.3. Audit Controls

AWARDS has an audit trail that allows the System Administrator to monitor user activity for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in Section 6 of these policies and procedures:

a. Are capable of recording data access for specified users when requested by authorized management personnel;
b. Retain 'Read Only" Audit trail logs for five years

BCS will maintain and follow procedures to provide and maintain unique usernames to each new user of their project-level HMIS-compliant system. At minimum, this procedure must:

- Require users to log-into systems;
- Define a period of inactivity after which the user's workstation must be automatically logged out of the system and/or locked out of the computer, requiring a username and password to resume use of the project-level HMIS-compliant system;
- Require that any default passwords provided for initial entry into the application be changed on first use;
- Define how individual users' forgotten passwords will be reset and communicated to the user;
- Specify how unsuccessful login attempts will be handled and confirm that the project-level HMIS-compliant system will maintain an auditable record of all attempted logins. At maximum, 5 consecutive unsuccessful login attempts must lock a user out of the system for at least 30 minutes. BCS HMIS Administrators may manually restore access prior to end of the 30 minute period.

BCS remote access procedures states that any user granted remote access will be monitored and that a list of such users will be maintained by BCS. BCS will ensure the security of the system and the confidentiality of the data during collection, use and transmission.

2.5. Audit Controls

BCS will maintain and follow procedures to ensure that its project-level HMIS-compliant system maintains audit records of user activity, including attempted logins, searches conducted by each user, records altered by each user, and records added by each user. BCS will follow procedures to monitor these records regularly for security breaches or behavior inconsistent with the Privacy Policy outlined in Section 6 of these policies and procedures. BCS will conduct a monthly review of the audit records.

2.6. PII Management and Disposal

It is the policy of BCS that users are responsible for maintaining the security of all client data extracted from the Data Warehouse. Users may not electronically transmit any unencrypted client data across a public network. Users must maintain the security of all hardcopy PII. BCS is responsible for maintaining and following procedures related to data management.

2.6.1. Electronic Data Storage and Management

Procedure: All connections to the Foothold AWARDS HMIS for purposes of uploading data will be made over SSL connections. Any other transmission of HMIS data containing PII will be limited to secure direct connections or, if transmitted over the internet, the data will be encrypted using a 128-bit key. If PII is emailed, it must be encrypted.

It is the policy of BCS that all hard drives and removable media on which PII is stored are encrypted. Under no circumstances will users store PII on any personally owned media; users may not place PII on a work-owned USB drive for personal use. AWARDS end users subject to NYC DHS policies are advised that this policy does not include any use that is unlawful, violates the City's Conflicts of Interest rules or other applicable rules and regulations, or is specifically prohibited by this policy or another applicable agency policy.

Critical data and removable data devices (USB drives, CDs, external drives, etc.) must be protected by appropriate physical means from modification, theft, or unauthorized access.

Such records and confidential information contained therein remain subject to these policies and procedures. When these media have reached the end of their useful life, the data will be disposed consistent with the procedures outlined in Section 4.7.3 of these policies and procedures.

2.6.2. Hard Copy Data Storage and Management

Hardcopies of data stored or intended to be stored in the Data Warehouse or a project-level HMIS - compliant system, regardless of whether the data has yet been uploaded to the Data Warehouse, 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 End 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 BCS 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 Section 6 of these policies and procedures.

5. If records are being transmitted from one location to another, they must be placed in sealed envelopes and a receipt shall be obtained documenting the delivery of said records.
6. Faxes or other printed documents containing PII shall not be left unattended.
7. Fax machines and printers shall be kept in secure areas.
8. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
9. When finished faxing, copying or printing all documents containing PII should be removed from the machines promptly.

Such records and confidential information contained therein remain subject to these policies and procedures. When these materials have reached the end of their useful life, the data will be disposed consistent with the procedures outlined in Section 4.7.3 of these policies and procedures.

2.6.3. Electronic and Hard Copy Disposal

BCS will establish policies and procedures for proper disposal of electronic and hard copy PII.

The HMIS Lead, in managing the Data Warehouse, will take the following steps when disposing of media (e.g., servers, workstations, mobile devices removable storage etc.) which contain PII:

1. Providers shall do or complete the D 5220-22.M and the Gutman Wipe.
2. Providers shall sanitize hardware through crushing, shredding, incineration, or melting.
3. Providers shall sanitize hardware it to a Pseudo Number Random Generator PRNG Stream with eight passes.

Hard copy records containing PII must be disposed of through means such as cross cut shredding and pulverizing.

BCS staff and the HMIS Lead will dispose of records in accordance with the Record Retention Schedule described in Section 6.10 of these policies and procedures.

2.7. Security Incidents

Policy: All HMIS Users are obligated to report suspected instances of noncompliance with these policies and procedures that may leave HMIS data vulnerable to intrusion. The HMIS Lead is responsible for reporting any security incidents involving the real or potential intrusion of the Data Warehouse to the Steering Committee. BCS is responsible for reporting any security incidents involving the real or potential intrusion of its project-level HMIS-compliant system to the HMIS Lead.

2.7.1. Reporting Threshold

BCS AWARDS users will report any incident in which unauthorized use or disclosure of PII has occurred.

BCS users will report any incident in which PII may have been used in a manner inconsistent with the BCS Privacy or Security Policies. Security breaches that have the possibility to impact the NYC HMIS must be reported to the HMIS Administrator.

BCS will maintain and follow procedures related to thresholds for security incident reporting.

2.7.2. Reporting Process

BCS users will report security violations to their BCS HMIS Administrator and Security Contact. The BCS HMIS Administrator will report violations to the HMIS Lead Security Officer (or designee).

FTS will regularly check the Data Warehouse for security breaches and failures and any such breaches or failures will be communicated to the HMIS Lead Security Officer and System Administrator.

The HMIS Lead Security Officer, in cooperation with the System Administrator, will review violations and recommend corrective and disciplinary actions to the Data Management Committee and the Steering Committee, as appropriate.

BCS will maintain and follow procedures related to internal reporting of security incidents.

3. Disaster Recovery

Policy: DHS's Emergency Preparedness and Operations Unit, housed within the Division of Security manages all major agency-wide emergencies, citywide coastal storm sheltering emergencies, and associated emergency planning activities. In the event of an emergency, in addition to performing the duties outlined by the Emergency Preparedness and Operations Unit, the HMIS Project System Administrator will coordinate with FTS to ensure the Data Warehouse is functional and that data is restored according to the procedures outlined in the security plan. BCS has a plan for maintaining and recovering access to its own data.

3.1. HMIS Lead

Procedure: DHS participates in NYC's Continuity of Operations Planning (COOP) program, which ensures City agencies can continue providing vital public services in the event of an emergency. In October 2007, Mayor Bloomberg signed a law requiring all City agencies to develop standardized COOP plans. DHS has an internal COOP team to survey its critical functions, and uses the COOP software to help them determine how to support or reinforce these functions during emergencies.

In June, 2006, Mayor Bloomberg and the Office of Emergency Management (OEM) unveiled the City's revised Coastal Storm Plan (CSP)-the plan that is used to respond to any coastal storm that may impact the City. DHS assisted OEM with the emergency shelter planning components of the CSP, and has been tasked to lead many of the planning initiatives necessary to ensure that the Emergency Shelter system is robust and operational.

3.2. FTS

Procedure: Should access to the DW be interrupted, FTS will contact the System Administrator, who will communicate this message to the BCS staff. The Data Warehouse is protected according to the terms of the security plan and all data will be restored to the most recent available backup day following any disaster that results in loss of data.

3.3. BCS

Procedure: BCS has a plan in place for maintaining and recovering access to its own data. Should a BCS's project-level HMIS-compliant system experience an interruption or loss of data that will

have implications for the NYC HMIS, the BCS HMIS Administrator must contact the HMIS Lead System Administrator within 5 business days.

4. Privacy Policy

4.1. Goal and Purposes

BCS has its own Privacy Policy to ensure that all required client data will be captured and to maintain the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.
Foothold AWARDS meets the privacy requirements established in HUD's privacy standards.

4.2. Applicability

Policy: The HMIS Privacy Policy applies to the HMIS Lead, the Data Warehouse, BCS staff, their project-level HMIS-compliant systems, and any person accessing any HMIS data. BCS projects that are subject to the privacy rules established under the authority of the Health Insurance Portability and Accountability Act (HIPAA) are exempt from this policy.

Procedure: The boundaries of the HMIS implementation are described in Section 1 of these policies and procedures.

The HMIS Lead and BCS staff will uphold Federal and State Confidentiality regulations to protect client records and privacy. If BCS is covered by more stringent regulations, the more stringent regulations will prevail. Any project not subject to the HMIS Privacy Policy will be identified in the BCS's Participation Agreement.

4.3. BCS Policy

BCS is responsible for maintaining a privacy policy and certifying that each participating project is in compliance with the NYC CCoC HMIS Privacy Policy. BCS's Administrator will be responsible for reviewing its privacy policy and the BCS Agreement must include certification of consistency with these privacy policies. BCS may require more rigorous privacy standards, but they must at minimum meet the privacy standards set forth in this document and must not conflict with this privacy policy. In addition, BCS must maintain documentation about changes to their privacy policies.

Procedure: BCS has its own privacy policy.

A BCS's Privacy Notice will:

- Specify all potential uses and disclosures of client personal information.
- Specify the purpose for collecting the information.
- Specify the time period for which the data will be retained at the organization and the method for disposing of it or removing identifiers from personal information that is not in current use 7 years after it was added to the HMIS or last changed.
- State the process and applicability of amendments, and commit to documenting all privacy notice amendments.
- Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process.

- Allow the client the right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand.
- Specify a procedure for accepting and considering questions or complaints about the privacy policy.

4.4. Compliance Review

BCS is responsible for conducting a review annually and certifying that each participating project is in compliance with the NYC CCoC Privacy Policy and HUD standards. The CCoC, through the HMIS Lead Agency, retains the right to conduct site visits to check compliance with the privacy policy and to verify self-certification of BCS.

Procedure: Each year BCS will be required to self-certify via a checklist or other document provided by the HMIS Lead that they are in compliance with the privacy policies adopted by the NYC HMIS. Each BCS staff will indicate that they are in compliance with the HMIS Lead privacy policy on the Administrative/Software compliance document annually. This document is provided in Appendix D. This form will be included as an exhibit to the Participation Agreement (see Section 3 of these policies and procedures). Failure to submit this form within 30 days of its due date in any given year will be considered to be a violation of the terms of the Participation Agreement and the BCS will be subject to the procedures described in Section 3.7.3 of these policies and procedures.

Each BCS will indicate in the Administrative/Software compliance document whether or not it has either:

- Adopted the minimum standard privacy policy (provided in Appendix H to these policies and procedures) as their own, or
- Adopted a different privacy policy that meets the requirements outlined in the HMIS Lead privacy policy.

In the event that the BCS has adopted a different privacy policy, the BCS will be expected to attach a copy of the policy to the Administrative/Software compliance document. If no policy has been adopted at the time of execution of the Participation Agreement, or at the time of the annual certifications thereafter, the BCS must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. An updated Administrative/Software compliance document indicating full compliance will be provided to the HMIS Lead by the target date or the BCS will be considered to be in violation of the terms of the Participation Agreement and will be subject to the procedures described in Section 3.7.3 of these policies and procedures.

4.5. Privacy Policy Notice

Policy: The HMIS Lead and BCS must ensure that their privacy policies are readily accessible to clients and the public.

4.5.1. Public Access

BCS will post the privacy policy in BCS website.

4.5.2. Informed Client Consent

BCS will post a sign at each intake desk or other location where data collection occurs explaining the reasons they ask for HMIS data. The sign will include the following language:

We collect personal information about homeless individuals in a computer system called a Homeless Management Information System (HMIS) for reasons that are discussed in our privacy policy. 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 individuals, and to better understand the needs of homeless individuals. We only collect information that we consider to be appropriate. If you have any questions or would like to see our privacy policy, our staff will provide you with a copy.

4.5.3. Accessibility

BCS will provide required information in Spanish and any languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the organization.

BCS privacy policy must include a provision stating that they will make reasonable accommodations for persons with disabilities throughout the consent, intake, and data collection processes. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability.

4.6. HMIS Data Use and Disclosure

Policy: The confidentiality of the data collected in the HMIS must be protected. BCS must collect data by legal and fair means, consistent with Section 6.6.2 of these policies and procedures. The HMIS Lead and BCS may only collect, use, and disclose these data for the specific purposes and reasons defined in this section.

The HMIS Lead collects HMIS data from homeless service organizations that upload data into a Data Warehouse. These data are collected only for specific purposes of carrying out the duties of BCS, the HMIS Lead, or when required by law. HMIS data may only be collected, used, or disclosed for activities described in this section. The HMIS Lead or BCS may or may not make any of these uses or disclosures of HMIS data. The HMIS Lead requires that individuals that seek assistance from BCS are notified that data collection, use, and disclosure will occur. By uploading data to the Data Warehouse, the BCS verifies that individuals have provided the BCS with consent to the use or disclosure of their HMIS data for the purposes described below and for other uses and disclosures that the HMIS Lead determines to be compatible with these uses or disclosures:

- To provide or coordinate individual case management services;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to audit, personnel oversight, and management functions;
- To produce aggregate-level reports regarding use of services;
- To create de-identified (anonymous) information;
- To track project-level outcomes;
- To identify unfilled service needs and plan for the provision of new services;
- To conduct a study or research project approved by DHS IRB,;

- When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
- To avert a serious threat to health or safety if:
  - The use or disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
  - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
- To report about an individual reasonably believed to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three circumstances:
- Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
- If the individual agrees to the disclosure; or
- To the extent that the disclosure is expressly authorized by statute or regulation and either of the following are applicable:
  - The BCS believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
  - If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the HMIS data for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; When such a permitted disclosure about a victim of abuse neglect or domestic violence is made, the individual making the disclosure will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
- In the exercise of professional judgment, it is believed that informing the individual would place the individual at risk of serious harm; or
- It would be informing a personal representative (such as a family member or friend), and it is reasonably believed that the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.
- To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the law enforcement official makes a written request for HMIS data that:
  - Is signed by a supervisory official of the law enforcement agency seeking the HMIS data
  - States that the information is relevant and material to a legitimate law enforcement investigation;
  - Identifies the HMIS data sought;
  - Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
  - States that de-identified information could not be used to accomplish the purpose of the disclosure.
- If it is believed in good faith that the HMIS data constitutes evidence of criminal conduct that occurred on the BCS's premises;

- In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the HMIS data disclosed consists only of name, address, date of birth, place of birth, social security number and distinguishing physical characteristics; or If:
    - The official is an authorized federal official seeking HMIS data for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and
    - The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.
- To third parties for the following purposes:
    - To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and
    - To permit third party research firms and/or evaluators to perform research and evaluation services, approved by DHS IRB, in connection with the projects administered by the HMIS Lead and the BCS;
    - Provided that before client-level HMIS data are disclosed under this subsection, the third party that will receive such client-level HMIS data and use it as permitted above must first execute a Data Use & Disclosure Agreement requiring such third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the current Department of Housing and Urban Development Homeless Management Information Systems Data and Technical Standards, which such standards and provisions are reflected herein.

The HMIS Lead may share client level HMIS data with contracted entities as follows:

- The BCS originally uploading the data to the NYC HMIS;
- Outside organizations under contract with the HMIS Lead or other entity acting on behalf of the CCoC for research, data matching, and evaluation purposes. The results of this analysis will always be reported in aggregate form; client level data will not be publicly shared under any circumstance.

Any requests for reports or information from an individual or group who has not been explicitly granted access to the NYC HMIS will be directed to the CCoC Steering Committee. No individual client data will be provided to meet these requests without proper authorization.

Before any use or disclosure of PII that is not described here is made, the HMIS Lead or BCS wishing to make the disclosure will seek the consent of any individuals whose PII may be used or disclosed.

4.7. Access and Correction

Policy: Clients whose data is collected in HMIS may inspect and have a copy of their HMIS record by requesting it from BCS that originally collected the information. The HMIS Lead requires that BCS establish a policy to manage such requests and to explain any information that a client may not understand.

Procedure: BCS will describe in its privacy policy how it will manage requests from clients for correction of inaccurate or incomplete HMIS records. This policy will allow for a client to request to see their HMIS data or request that data be removed from the HMIS. Nothing in this section is intended to indicate that a BCS is released from any obligation by any funder to collect required data elements.

If BCS agrees that the information is inaccurate or incomplete, they may delete it or they may propose to mark it as inaccurate or incomplete and to supplement it with additional information. Any such corrections applicable to the data stored in the Data Warehouse will be made at the time of the next upload.

A record of these transactions will be kept by the BCS HMIS Administrator. In response to requests to view his/her data in the HMIS, the BCS HMIS Administrator or case manager will provide a copy of the requested data within a reasonable time frame to the client.

BCS Supervisory staff are permitted to establish reasons for denying client requests for inspection of HMIS records. These reasons are limited to the following:

If the information was compiled in reasonable anticipation of litigation or comparable proceedings;

- If the record contains information is about another client or individual (other than a health care provider or homeless provider) and the denial is limited to the section of the record containing such information;
- If the information was obtained under a promise of confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; or
- Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If BCS denies a request for access or correction, BCS will explain the reason for the denial and also maintain documentation of the request and the reason for the denial.

BCS may reject repeated or harassing requests for access to or correction of an HMIS record.

4.8. Data Retrieval and Sharing

Policy: As the HMIS Lead Agency, DHS Planning, Development & Grants unit, and associated staff, has access to retrieve all data in the NYC HMIS. No other staff member of DHS has access to client-level data. DHS must protect client confidentiality in all reporting.

BCS staff may share PII with each other, provided they have executed a data sharing agreement outlining roles, responsibilities, parameters of data sharing, and the steps that will be taken if one party withdraws from the data sharing agreements.

Procedure: HMIS as implemented in NYC is a system which can provide reports required by HUD, the Continuum of Care, and other stakeholders at a reporting level that does not identify individuals but can provide accurate statistical data including, numbers served, trend assessments, and non-duplicated statistical reports based on data entered into the NYC HMIS by BCS. Data from the NYC HMIS will be used to produce these COC and local level statistical reports required by HUD

and will be used in various HUD applications and reports. These uses are included in the uses and disclosures described in Section 6.7 of these policies and procedures.

Data sharing between BCS staff for the purpose of coordinating services is also included in the allowable uses and disclosures described in Section 6.7 of these policies and procedures.

4.9. Record Retention Schedule

Policy: The HMIS Lead, consistent with standards developed by HUD, will dispose of or de-identify PII not in current use seven years after the information was created or last changed. The HMIS Lead may keep information for a longer period if required to do so by an applicable statute, regulation, contract or other requirement.

Similarly, BCS staff are required to establish a policy to dispose of or de-identify PII not in current use seven years after the information was created or last changed unless prohibited from doing so by an applicable statute, regulation, contract or other requirement.

Procedure: The HMIS Lead will coordinate with FTS to ensure that data in the Data Warehouse is retained according to the policies and procedures. BCS will include a provision in its policies and procedures to comply with this policy.

4.10. Grievance

Policy: Concerns related to the HMIS Privacy Policy may be raised according to the procedures outlined in Section 2.6 of these policies and procedures. BCS will establish a policy and regular process for receiving and reviewing complaints from clients about potential violations of the policy.

Procedure**:** BCS will report any violation of their privacy policy to the HMIS Lead. In addition to any actions taken by BCS to sanction the employee, depending on the frequency, prior training, severity, intent, etc., of the violation, the HMIS Lead may report the findings to the Steering Committee or law enforcement, as appropriate, for further action. Such action may include,

- Suspension of system privileges; or
- Revocation of system privileges.

Sanctions can be appealed to a group comprised of the Steering Committee and any necessary ad hoc members.

5. Data Quality Plan

5.1. Goal

Data from the NYC HMIS will be used to document Continuum of Care needs, performance, and to document services provided to the homeless. The NYC HMIS will provide statistics and outcome measures for reports to HUD, the Steering Committee, and other stakeholders.

For NYC HMIS to be able to provide accurate and timely information, HMIS participation must be maximized, data must be collected by BCS regularly, completely, and accurately, and data must be

uploaded to the NYC HMIS in a timely manner. This will permit the HMIS Lead to produce reports related to the annual evaluation, the Housing Inventory Count, the Point in Time Count, and the Annual Homeless Assessment Report. In addition, improved participation and data quality will enhance the competitiveness of the CCoC in the annual HUD competition.

The goal of these HMIS Data Quality policies and procedures is to standardize expectations and provide guidance to HMIS participating projects on the extent and quality of data entered into the NYC HMIS so as to be able to draw reasonable conclusions about the extent of homelessness and the impact of homeless services.

5.2. HMIS Participation Thresholds

Policy: 100% of all programs funded by ESG, CoC, SHP, S+C, SRO Mod Rehab, HOPWA, GDP, VA Community Contract, SSVF, and SAMHSA PATH projects are required to participate in HMIS, as stated in Section 1 of these policies and procedures. In addition, the CCoC aspires to have 100% of all projects primarily dedicated to serving homeless persons (in other words, continuum providers) participate in HMIS.

Procedure: The HMIS Lead will maintain a listing of all continuum lodging and services projects' participation in HMIS. On a quarterly basis, the status of each project will be updated and reported to the Steering Committee. Each project will be indicated as "fully participating," "uploading incomplete data," "implementing," or "not yet participating."

5.3. Minimum Required Data Elements

Policy: BCS is required to collect and submit all required program descriptor data elements to the HMIS Lead prior to initial setup in the HMIS, at the time of any change to any program descriptor data element (e.g. number of beds/units operated or type of households served) and annually thereafter. In addition, BCS is required to upload records on all clients participating in each HMIS participating project. A record comprises, at minimum, all Universal Data Elements and Program-Specific Data Elements applicable to the project type and meets the accuracy, completeness, and timeliness standards outlined in these policies and procedures. The required data elements, along with detailed definitions and explanations are provided in NYC HMIS Data Dictionary, included as Appendix I to these policies and procedures.

Procedure: BCS will provide all required program descriptor data elements for each participating project via the Project Information Form incorporated into the Participation Agreement as described in Section 3 of these policies and procedures. The Project Information Form is provided in Appendix F.

BCS will upload complete records on all clients in each HMIS participating project to the Data Warehouse at least once per month. The HMIS Lead will maintain the NYC Data Standards consistent with HUD's most current HMIS Data Standards. The HMIS Lead System Administrator will be responsible for communicating any updates to the NYC Data Standards to each BCS HMIS Administrator and for providing trainings to them to ensure that they, in turn, are able to train their end users on the changes. The full HUD Data Standards can be found on HUD's Homelessness Resource Exchange at http://www.hudhre.info/.

5.4. Data Collection and Upload Standards

Policy: The HMIS Lead is responsible for the overall HMIS data quality. In an effort to maintain that quality, the HMIS Lead has established data quality thresholds for participating projects to meet the terms of their Participation Agreements. BCS is responsible for developing and implementing policies to ensure that its end users are entering data into the project-level HMIS-compliant system in a timely, complete, and accurate manner. The HMIS Lead and BCS are jointly responsible for ensuring that project data in the HMIS meets the thresholds outlined in this section. In order to develop consistency in data collection processes and develop capacity among end users, the Data Management Committee and the HMIS Lead may establish an HMIS user group.

5.4.1. Timeliness

The purpose of timeliness is to ensure access to data when it is needed – either proactively (for planning or monitoring purposes, or to meet reporting requirements) or reactively (in response to a request for information or to respond to inaccurate information).

Standard:

All HMIS participating projects will ensure entry of data for new clients, services provided to new and existing clients, and exits for each month, that are uploaded to the NYC Data Warehouse by the 10th business day of the following month. Any corrections that may need to be made to address technical or data quality issues must be resolved no later than the 20th business day of the following month.

BCS will develop and implement a policy requiring that all client data be entered into the project-level HMIS-compliant system within three business days of a client interaction. Data required to be collected at entry according to current HUD HMIS Data Standards will be entered within three business days of a client's entry date. Data required to be collected at exit according to current HUD HMIS Data Standards will be entered within three business days of a client's exit date. Data required to be collected at least once every three months during enrollment according to current HUD HMIS Data Standards will be entered within three business days of the client reaching the three-month period of enrollment, if applicable. Data required to be collected at least annually during enrollment according to current HUD HMIS Data Standards will be entered within three business days of the client reaching the one-year period of enrollment, if applicable. Data required to be collected at every contact or service provision according to current HUD HMIS Data Standards will be entered within three business days of the contact/service. Changes to active client data must comply with the HUD Data Standards, but should occur within three business days of learning of a material change.

BCS will have the policy done by Sept. 13th 2013.

5.4.2. Completeness

The purpose of completeness is to ensure sufficient data on clients, their demographic characteristics, and service use to facilitate confident reporting and analysis on the extent and characteristics of the homelessness including:

- Unduplicated counts of clients served in the continuum of care;
- Patterns of use of people entering and exiting the homeless assistance system; and
- Evaluation of the effectiveness of homeless systems.

Standard:

The goal is that ALL projects participating in the NYC HMIS will have complete data; however, residential projects with less than 75% data completeness and SSO/Outreach projects with less than 50% data completeness will be considered to be in violation of their Participation Agreement and will be subject to the process described in Section 3.7 of these policies and procedures.

This will be evaluated by the HMIS Lead on a quarterly basis and will be calculated as an overall percentage of all required data fields for all clients active during the quarter. The HMIS Lead will provide a quarterly report to BCS detailing the number of clients added in the quarter, active in the quarter, and the missing/ don't know/ refused rate for each data element for clients active during the quarter. This report will be the basis of determining if the project is meeting the standards and is intended to assist the BCS in identifying and correcting missing data in its project-level HMIS-compliant system and discrepancies between the project-level HMIS-compliant system and the Data Warehouse (if any). In addition, the HMIS Lead will provide a length of stay and bed utilization report to all lodging projects in an effort to highlight missing exit data (high rates of longer-than-expected lengths of stay and/or overutilization of beds can indicate that clients are not being exited appropriately).

The expectation is that there is no missing data. In the event data was not collected, however, the "don't know" and "refused" responses should not be used. These response options are expected to indicate that the client did not know a response or that the client refused to respond, not that the case manager or other user did not know the response or refused to collect. All Universal and Program Specific Data elements are required, and so it is expected that it is very unlikely that any field would be left blank.

5.4.3. Accuracy

The purpose of accuracy is to ensure that the data housed in the NYC CoC HMIS is the best possible representation of reality as it relates to homeless people and the projects that serve them. Accuracy is determined by assessing the truthfulness by the client, the accuracy of the data collected by staff, and the accuracy of the data entered into the system by the staff. BCS is responsible for making these assessments. In the Data Warehouse, accuracy is assessed by verifying consistency across all forms of reporting: NOFA Project Applications, APR, NYC CCoC Evaluation and any other similar reports.

Standard:

The goal is to make sure HMIS data is entered correctly and can be verified with documentation. BCS will regularly check the accuracy of the information provided against other reliable sources and perform checks on data elements such as date of birth (e.g. no negative ages or dates after the present entered for this field), veteran status (children are not categorized as veterans), disability status (someone who receives SSI is not categorized as having no disabilities).

BCS will develop and implement an internal business process for conducting logic checks (such as those suggested in the paragraph above) on the data in its project-level HMIS-compliant system and regularly comparing universal and program specific data elements to available paper records and updating/correcting missing or inaccurate data. BCS will develop and implement an internal process that engages both intake and data entry staff to ensure collaboration and communication focused on input of accurate client data into the HMIS system.

5.5. Data Quality Monitoring

BCS is responsible for addressing any issues identified through the process of this monitoring prior to the next scheduled upload to the Data Warehouse. Any BCS failing to meet the data quality standards as averaged over the calendar year will be considered to be in violation of the terms of the Participation Agreement and will be subject to the procedures described in Section 3.7.3 of these policies and procedures.