BronxWorks Confidentiality Policy

I. Introduction:

A. Background:

1. BronxWorks is a not-for-profit community-based agency whose mission is to help individuals and families improve their economic and social well-being. To do this, BronxWorks provides direct, hands-on help, community outreach, education, and advocacy. In order to effectively provide services and coordinate the receipt of these services, BronxWorks collects and shares information within the agency in furtherance of BronxWorks’ mission.

2. BronxWorks may disclose information to third parties in order to assist in the administration of these services after receiving appropriate consent from the client. Additionally, BronxWorks may be required to disclose information to third parties in other cases (e.g. Court Ordered subpoena, suspected child abuse or neglect, or if client is a danger to himself/herself or others). In such cases, BronxWorks aims to ensure that the information disclosed is appropriate and that the information is disseminated in a controlled manner in accordance with any and all applicable laws.

3. This document is the Confidentiality Policy (“Policy”) for BronxWorks and provides standards and guidelines for the use, disclosure, and security of all BronxWorks Client information. Policy applies to all BronxWorks staff, volunteers, and affiliates (e.g. subcontractors).

B. Scope:

1. Policy applies to all personal communication regarding Confidential Information whether on the job or off the job and extends to both current employees and Confidential Information obtained by former BronxWorks employees.

2. Policy applies to all devices, applications, systems, and records which contain Confidential Information.

3. Policy applies to all records—electronic or paper—made and retained by BronxWorks.

4. All existing confidentiality policies or contracts with individual program funders supersede Policy. All new or updated contracts with funders specific to individual programs should be reviewed by General Counsel prior to agreement. If an existing or updated policy does not address an area covered in Policy, Policy shall be applied.

C. Applicable Law and Policies:

1. Policy is governed by the applicable Federal, State and Local laws including but not limited to the New York Social Services Law and its implementing

2. Additionally, Policy incorporates all previous BronxWorks confidentiality policies agreed upon during the hiring process (i.e. Electronic Communication Confidentiality Policy) and must be used in conjunction with all program/funder specific confidentiality policies and does not supersede these policies.

3. All licensed professionals shall strictly abide by their specific Code of Ethics (e.g. National Association of Social Worker’s Code of Ethics or American Medical Association’s Code of Medical Ethics) (see attached). Failure to comply may result in review by the appropriate governing panel and possible termination of the employee’s license.

D. Key Definitions:

1. For the purpose of Policy, the term “Client” refers to an individual or family applying for or who has previously applied for or is receiving or has formerly received BronxWorks services.

2. The term “Confidential Information” refers to the following Client information:
   a. Name
   b. Date of birth
   c. Social Security Number, DHS Shelter placement
   d. Address
   e. Medical
   f. Public Assistance (PA) Case or Client Identification Number
   g. PA, Supplemental Security Income (SSI), Social Security Disability (SSD), or other benefit or entitlement information
   h. Any other information obtained in the course of administering or accessing Client for BronxWorks services
   i. DHS Case or Housing Assistance (HA) Number used in combination with a-i above

3. The term “Record” refers to any papers or electronic file or document which contains Confidential Information.

4. For the purpose of Policy, the term “Funder” refers to governmental organizations with whom contracts currently exist and applies to all future contracts with governmental organizations.

5. Additionally, Confidential Information applies to BronxWorks employees as follows:
   a. personal information about employees, such as salary information, performance appraisals, and medical information
   b. any work related information which is provided in confidence on behalf of
BronxWorks, such as information of a personal nature relating to BronxWorks clients, program participants and/or residents and program contract information

II. **Privacy and Confidentiality**

A. **Ownership and Use of Confidential Information**

1. BronxWorks employees may only collect or use Confidential Information to perform functions, activities, or services directly related to the administration of BronxWorks programs.

2. Access to Confidential Information shall be restricted to those employees who need such information to perform their official duties in connection with the administration of BronxWorks programs. Access to Confidential Information shall be limited to only those staff whose duties require access and is limited to Confidential Information which pertains to Clients directly served by that staff member.

3. BronxWorks owns all Confidential Information collected by its employees or volunteers unless specified otherwise in an existing funder contract. BronxWorks owns all Records created and maintained in connection with the administration of BronxWorks programs unless specified otherwise in an existing funder contract.

4. For BronxWorks programs which are required to enter Confidential Information into an electronic database maintained by the respective program’s governmental funding agency, that Confidential Information is owned by that government agency if specifically outlined by funder’s contract.

B. **Disclosure of Client Information**

1. **Permitted Disclosures**

a. Section 136 of the New York Social Services Law and 18 N.Y.C.R.R. Part 357 prohibits the disclosure of Confidential Information with limited exceptions.

b. Policy prohibits a BronxWorks employee from disclosing Confidential Information or any part of Client’s Record to a third party without explicit consent unless approved by General Counsel or unless such information is being released pursuant to

   i. a supervisor or manager to whom employee reports within the agency and in order to perform activities directly related to the administration of BronxWorks services or referrals
ii. reports to funders which Client has been notified of and has provided written consent (e.g. an existing contract, data-match, or data exchange agreement)

iii. a routine response to an Oversight agency such as OTDA, DHS, ACS, DOH, etc. which must be accompanied by written consent from Client

iv. All other requests for Confidential Information pursuant to the Freedom of Information Law (“FOIL”) including Administrative or Judicial subpoenas; Federal, State, and Local Law Enforcement officers; and Court-Ordered discovery should be referred to General Counsel prior to the release of Confidential Information.

v. BronxWorks staff must provide General Counsel with agreements for data-matches or data-exchanges for review before such agreements are executed.

2. Mandated Reporters:

Nothing in Policy prevents a BronxWorks employee from reporting known or suspected instances of physical or mental injury, sexual abuse, contract or exploitation, or negligent or maltreatment of a child to the appropriate agency or officials.

3. De-identified Information:

Policy does not prohibit the release of de-identified information for Data Exchanges/Matches or Program Evaluations with program funders or Federal, State, and Local government agency. De-identified Information does not contain the following Client information:

   a. Name
   b. Social Security Number
   c. Address
   d. Shelter Placement or Address
   e. HRA or Social Security Client Identification Number, or
   f. PA Case Number

4. Subpoena Policy:

Employees must inform their supervisor immediately if a case record is subpoenaed. The supervisor must, in turn, inform his/her supervisor so that the subpoenas can be jointly handled by the Assistant Program Director and the General Counsel.

Moreover, employees must inform the supervisor whenever police make inquiries about their clients or appear at BronxWorks offices with arrest and/or search warrants. The supervisor must, in turn, inform the Assistant Executive Director and General Counsel. If the situation arises during normal work days/hours, the Program and Assistant Executive Director should contact the Administration office so
that the inquiries or warrants can be handled jointly with the General Counsel.

Under no circumstances are employees to relinquish case records or confidential information to anyone other than his/her supervisor or management personnel. Employees may not release the information until they have received authorization from the Program Director, Department Director and the General Counsel.

5. Employee Discipline:

The unauthorized use or disclosure of Confidential Information may result in any and all of the following:

a. the loss of use or limitations on the use of office and technology resources;
b. financial liability for the cost of such use;
c. disciplinary and other adverse employment actions, up to and including dismissal;
d. civil and/or criminal penalties

A. Client Requests for Records:

1. BronxWorks will release Records to Client or his/her representative so long as Client or his/her legal representative makes his/her request in writing, which is accompanied by a release that has been signed by Client unless Client is legally incapacitated or deceased.

2. Before providing Client with his/her Record or other files containing Confidential Information, BronxWorks employees shall remove the following items, which should not be retained in Records or Client files:

a. Emails issued by program funder staff
b. Intra-Inter agency memoranda
c. Rules of Practice
d. Information contained from confidential external sources
e. Documents marked “draft,” “privileged,” or “confidential”
f. Any note containing information that could be harmful to the wellbeing of the client or his/her family/community either physically or emotionally as deemed appropriate by state and federal law

3. Requests for Record in connection with Involuntary Transfer/Discharge Hearings, State Fair Hearings or other Administrative or Judicial proceedings should be referred to General Counsel immediately but no later than 24 hours after the request for such information has been made. General Counsel will track and respond to such requests.

III. Security

A. General Provisions:
1. Record shall be kept in individual locked files or in rooms that are locked when Record is not in use which shall be maintained by the appropriate program supervisor.

2. When in use, Record shall be maintained in such a manner as to prevent exposure of Confidential Information to anyone other than the authorized party directly utilizing the Record.

3. BronxWorks employees shall not remove Record or other information from their places of business without permission from appropriate supervisory staff. In such cases, all efforts to safeguard Confidential Information should be made (see A4).

4. When exempt staff (e.g. salaried employees) remove Record from their places of business after receiving supervisory approval in order to work from home, the Record shall be maintained in a secure location and staff must not disclose the Confidential Information contained in Record except as permitted by Section II of this Policy. All elements of Policy shall remain in effect and applied strictly to prevent inappropriate disclosure of Confidential Information.

5. Record shall be transmitted from one location to another in sealed envelopes marked “confidential” and a receipt shall be obtained documenting delivery of said Record.

6. All e-mails either sent to internal contacts or external contacts shall be marked confidential.

7. No client information provided via e-mail to an external agency shall be included in the body of an e-mail. All confidential information as defined in Policy must be attached in an encrypted document.

8. Client interviews shall be conducted at a location and in a manner which maintains privacy and confidentiality.

9. Users who have access to systems containing Confidential Information shall protect and secure their passwords. Users shall not copy Confidential Information on to portable media for personal use, sent to personal e-mail, or make copies of Confidential Information for use outside of the office unless this action is authorized by the employee’s manager. Users shall change their passwords as directed. Users shall not share their passwords.

10. BronxWorks appointed “superuser” or administrators must terminate access to electronic databases, ensure that all keys to areas containing Confidential Information are returned, and that all points of access are no longer accessible for employees no longer employed by the agency or on leave from the agency within two business days of the employee’s last day.

11. BronxWorks non-exempt employees shall not access BronxWorks e-mail or databases maintained by BronxWorks or by funders remotely unless approval has been granted by employee’s direct supervisor, program director, or General Counsel, and Policy should be strictly applied.

12. In order to maintain a domestic violence survivor’s confidential information, the following should be noted in the client’s case file and in any notes contained herein:
   - All information pertaining to domestic violence safety planning (i.e. a shelters business address or any confidential address of a survivor of domestic violence) should be clearly and boldly identified in a case record by preventive staff as “Confidential Information Due to Domestic Violence, Do Not Share.”
- The file shall not contain the name of the domestic violence shelter of a client but should instead state only the address—which should list the shelter’s P.O. Box

B. Controls for Paper Documents:

1. Programs governed by funder regulations in regard to the disposal of Record shall comply with all funder regulations.
2. BronxWorks staff shall not dispose of Record without authorization from the appropriate program funder and the Assistant Executive Director. If no program funder exists or program funder does not establish proper procedure for disposing of Record, staff must obtain authorization from Assistant Executive Director and General Counsel prior to the disposal or destruction of Record.
3. Record must be disposed of through confidential means such as cross cut shredding.
4. Faxes or other printed documents containing Confidential Information shall not be left unattended.
5. Fax machines and printers shall be kept in secure areas.

C. Provider Controls:

1. Employee Training and Discipline:

   BronxWorks shall:

   a. Require that each employee sign an Acknowledgment letter indicating that the employee has read, understood and agreed to fulfill all of the obligations contained in Policy which shall be returned and kept on file the day that employee adequately fulfills Confidentiality Training (C1.d) provided by BronxWorks
   b. Train its employees and use reasonable measures to ensure compliance with Policy including annual training
   c. Provide Privacy and Security training to each new employee within 30 days of employment and thereafter provide ongoing reminders of the privacy and security safeguards in Policy;
   d. Maintain records which include the name of each employee and the date on which he/she completed the initial Privacy and Security training;
   e. Retain Employee Acknowledgment letters and training records for inspection for a period of five years after the completion of training;
   f. Ensure that locations where Confidential Information is stored and/or processed, are secured by security guards or a monitored alarm system with security cameras 24 hours a day, 7 days a week
   g. Any questions or concerns regarding the release of Confidential Information should be directed to program directors for approval prior to the release of Confidential Information. If questions or concerns are not directly addressed by Policy or program specific funder agreements, program directors should direct any questions or concerns to General Counsel prior to release.
2. **General Computer Security Safeguards:**

For systems or devices containing Confidential Information, BronxWorks shall:

a. Protect by password, smart phones, laptops, tablets, or other portable telecommunications devices which users are not permitted to share.

b. Ensure that employee downloads only the minimum necessary amount of Confidential Information to a laptop, external drive, or other portable device when required for current business purposes and after receiving supervisory approval.

c. Ensure that workstations, laptops, and other systems that process and/or store Confidential Information have commercial, anti-virus, and Internet Security Software solutions, including but not limited to firewalls, malware, intrusion detection, etc. These solutions must be updated when new versions or releases become available.

d. Ensure current security patches have been deployed on workstations, laptops, and other systems that process and/or store Confidential Information.

e. Sanitize hardware by wiping all existing data from the computer hard drive.

3. **System Security Controls:**

All systems which contain Confidential Information and are administered by BronxWorks or Professional IT service entity hired by BronxWorks shall:

a. Require that users login to systems;

b. Retain a log of successes and authorization of user authentication and authorizations granted

c. Use role based access controls (user name and password) for all user authentication which enforces the principle of minimum privileges necessary

**IV. Notification of Unauthorized Use and Disclosure of Data**

A. If a BronxWorks employee discovers that there has been an unauthorized use or disclosure of Confidential Information, he/she shall report such incidents directly to General Counsel, the appropriate program director, and Assistant Executive Director in addition to reporting unauthorized access to individual program funders if specified in funder contracts.

B. **Initial Reporting Information:**

The following information must be collected and provided during the report:

1. Contact information
2. Physical location of the affected system(s)
3. Date/time of the incident
4. Nature of the data on the system (i.e., whether or not it contained restricted data)
5. Source of the compromise, if known (i.e., worm, virus, credential compromise, root kit, unauthorized verbal disclosure of Confidential Information, unauthorized access to remove systems including databases or e-mail, etc.)
6. Brief description of the incident
7. Any relevant logging information

Additional Provisions for CARES Users

1. DHS Records
   a. Department of Homeless Services (DHS) owns all Confidential Information collected by BronxWorks employees. DHS owns all Records created and maintained in connection with the administration of DHS programs.

   b. Employees who receive requests for Confidential Information should notify BronxWorks General Counsel and the Assistant Executive Director for follow up with DHS. Questions regarding the disclosure of Confidential Information should be directed to Legal at 212.361.7996.

   c. DHS will release Records to the Client or her representative so long as the Client makes her request in writing, which is accompanied by a release that has been signed by the client.
      • Before providing Clients with their Records or other files containing Confidential Information, BronxWorks employees shall remove the following items, which should not be retained in Records or Client files:
         a. Emails issued by DHS staff members
         b. Intra-Inter-agency memoranda
         c. Rules and Practices
         d. Information contained from confidential external sources, or
         e. Documents marked “draft,” “privileged,” or “confidential”

   d. DHS shall dispose of Records in accordance with DHS’ Record Retention Schedule.

   e. BronxWorks shall not dispose of Records without authorization from DHS.

   f. DHS Systems and Devices: All DHS systems, applications and devices are secured in accordance with standards and guidelines delineated by the New York City Department of Information Technology and Telecommunications (DoITT) covered under Citywide Information Security Policies.

2. BronxWorks Agency Responsibilities:
a. Sign an acknowledgment letter indicating that it has read, understood and agreed to fulfill all of the obligations contained in the DHS CARES Policy

b. Return the above Acknowledgment letter with an original signature no later than 5 business days from the date of the Acknowledgment letter;

c. Require that each employee sign an Acknowledgment letter indicating that he employee has read, understood and agreed to fulfill all of the obligations contained in the CARES policy

d. Provide Privacy and Security training to each new employee within 30 days of employment and thereafter provide ongoing reminders of the privacy and security safeguards in the CARES policy

e. Maintain Records which include the name of each employee and the date on which she completed the initial Privacy and Security training

f. Retain Employee Acknowledgment letters and training Records for inspection for a period of five years after the completion of training

g. Complete and return to a Security Assessment using a tool designated by DHS by a date specified by DHS

3. For systems or devices containing Confidential Information, BronxWorks shall:

    a. Encrypt laptops or other portable computer devices and media (e.g. USB thumb drives, external hard drives, CDs and DVDs) that process or store Confidential Information using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution. The keys to such encrypted files shall not be included with the transportable media which contains the Confidential Information. That information shall be communicated by telephone or email to the intended recipient.

    b. Ensure that workstations, laptops, and other systems that process and/or store Confidential Information have commercial, anti-virus, and Internet Security Software solutions, including but not limited to firewalls, malware, intrusion detection, etc. These solutions must be updated when new versions or releases become available.

    c. Ensure current security patches have been deployed on workstations, laptops, and other systems that process and/or store Confidential Information.

    d. Sanitize hardware through crushing, shredding, incineration, or melting when disposing of hardware (e.g., servers, workstations, mobile devices, removable storage, etc.) which contains Confidential Information.
e. Disallow remote access to a DHS application containing Confidential Information without prior authorization from DHS.

f. Ensure that remote access to any application containing Confidential Information is established via VPN or SSL-VPN only.

g. Ensure that all remote access is limited to the minimum privilege necessary to complete the task in question.

4. System Security Controls:

All systems which contain Confidential Information and are administered by BronxWorks or Professional IT service entity hired by BronxWorks shall:

a. Provide an automatic timeout after no more than 20 minutes of inactivity;
b. Display a warning banner stating that data is confidential, that system use is for business purposes only and that they agree to such terms by logging into the system;
c. Require that users login to systems;
d. Retain a log of successes and authorization of user authentication and authorizations granted;
e. Retain a log of all data changes and system accesses conducted by all users and at all levels;
f. Are capable of recording data access for specified users when requested by authorized management personnel;
g. Retain a log of system changes subject to review of authorized management personnel;
h. Use role based access controls (user name and password) for all user authentication which enforces the principle of minimum privileges necessary; and
i. Encrypt Confidential Information transmitted over networks outside of the City’s control using an end-to-end vendor product that is recognized as an industry standard in meeting the needs for the intended solution.

5. Audit Controls:

BronxWorks shall implement the following measures for systems which contain Confidential Information and are administered by BronxWorks or professional IT service entity hired by BronxWorks:

a. Conduct an annual system security review using a tool developed or designated by DHS’s Office of Information Technology (OIT);
b. Establish and maintain an automated audit trail, which identifies the user that initiated the request, data and time stamp for each access;
c. Retain “Read-Only” Audit trail logs for two years;
d. Routinely review system logs for unauthorized access;
e. Investigate anomalies in system usage; and
f. Exercise management control and oversight over the authorization of user access.

6. Notification of Unauthorized Use and Disclosure of Data

a. If a BronxWorks employee discovers that there has been an unauthorized use or disclosure of Confidential Information, he/she shall report such incidents to the employee’s respective program supervisor who shall notify the DoITT Help Desk 212.692.4357 and have the ticket assigned to DHS OIT as a priority 1 for investigation by OIT and Legal.

b. Initial Reporting Information:
The following information must be collected and provided during the initial call:
   i. Contact information
   ii. Physical location of the affected system(s)
   iii. Date/time of the incident
   iv. Nature of the data on the system (i.e., whether or not it contained restricted data)
   v. Source of the compromise, if known (i.e., worm, virus, credential compromise, root kit, etc.)
   vi. Brief description of the incident
   vii. Any relevant logging information (e.g., intrusion detection logs)