Executive Order No. 746 ***THE CITY OF NEW YORK***
October 3, 2017 ***DEPARTMENT OF SOCIAL SERVICES***

CONFIDENTIALITY POLICY

TO: Distribution I Through IX

FROM: Steven Banks
Commissioner

I. INTRODUCTION

The following agency-wide confidentiality policy applies to all of the New York City Department of Social Services (DSS) staff which includes the Human Resources Administration (HRA) and the Department of Homeless Services (DHS).

In addition, each Program and Administrative area is responsible for developing specific confidentiality procedures related to the nature of the work it performs and the particular issues that may arise as a result of this work. These procedures will be reviewed by the Office of Legal Affairs prior to issuance and annually to ensure consistency with overall Agency policy and with individual offices that may have overlapping program responsibilities.

This policy and relevant area-specific confidentiality procedures will be given to each new employee and discussed during orientation.

This policy is to be used as a general guidance on confidentiality issues. However, DSS staff who have questions about whether information is confidential and/or to whom it may be disclosed are advised to consult their supervisors or the HRA Chief Data Privacy Officer.

Definition of Confidentiality

A confidential document is defined as a document that contains any information that is private, or not for public dissemination. For purposes of this policy, information is considered confidential when a federal, state, or local law or regulation, or directive, memorandum, judicial decree, order, stipulation, settlement or some type of pre-existing agreement deems it confidential. Most Agency records and all client records are confidential.

Federal, state, and local privacy statutes apply to the release of, and/or sharing of, certain demographic information including, but not limited to, social security numbers, addresses, financial and marital and health insurance status.

Confidentiality laws and regulations also govern the use and disclosure of the following types of information:

1) an individual's health, including mental health, status or treatment history;
2) an individual's HIV status;
3) that the individual has been diagnosed or treated for substance and/or alcohol use;
4) domestic violence history, address information for survivors of domestic violence, and location of domestic violence emergency residential programs;
5) that a particular individual has applied for, has received or currently is a recipient of public assistance, food stamps, Medicaid or other public assistance benefits;
6) immigration status;
7) an individual's involvement with child welfare services;
8) any case specific information related to enforcement of child support obligations or the establishment of paternity;
9) ID NYC applicant/recipient information; and/or
10) Information concerning an applicant for or recipient of adult protective services.

A data security incident occurs when confidential information is disclosed to a third party without authorization, whether the disclosure is intentional or accidental. In some cases, a data security incident may be considered a breach. Whether a disclosure constitutes a breach is a legal determination to be made by the DSS Office of Legal Affairs. In the event of a suspected unauthorized disclosure of confidential information, DSS staff should immediately report the incident to their supervisors, and refer to the DSS Data Security Incident Procedure: What to Do in the Event of an Unauthorized Disclosure and Breach Prevention Measure, Procedure No. 17-09, September 14, 2017, for further guidance.

Disclosing confidential information is harmful to DSS's clients. It also harms the Agency by causing the public to lose trust in the Agency's ability to protect confidential information. Improper disclosure of confidential information is often a violation of the law, and can lead to financial liability for the Agency.

Additionally, any employee who improperly or illegally discloses confidential information may be subject to civil fines, a private lawsuit or a criminal prosecution, and may also be subject to employee discipline or discharge. Employees and other staff are advised that the improper disclosure of confidential information will be deemed to be outside the employee's official duties and the City of New York may refuse to legally defend or indemnify any employee found guilty or liable for violation of the confidentiality or privacy laws.

DSS staff authorized to have access to confidential information, who may have questions about disclosing confidential information, are advised to contact the DSS Chief Data Privacy Officer in the Office of Legal Affairs.

II. PROGRAM AND ADMINISTRATIVE PROCEDURE GUIDELINES

Individual Program or Administrative confidentiality procedures will vary depending upon the nature of the work of the unit. The following are some of the issues that should be addressed in area specific procedures:

- Removal of identifying information from emails, faxes, letterhead, return addresses, caller ID information, or voice-mails that may inadvertently disclose information about a client.
- Handling confidential files/information at staff desks or work stations.
- Handling confidential files/information when making copies.
- Developing/implementing security procedures for storing electronic and non-electronic confidential files.
- Handling personnel files that contain medical notes or other confidential information.

- Determining to whom staff may disclose information concerning clients, and the types of information that may be released.
- Determining the appropriate staff to handle confidential information.
- Establishing procedures to limit access to confidential information by non-permanent employees, such as temporary workers, consultants and interns.
- Referring requests for confidential information or records to the appropriate DSS office.
- Destruction of records.
- Authorizing staff to take work home or to other locations.
- Loss, theft or improper disposal of Agency equipment, i.e mobile devices, Agency issued cell phones, CDS, thumb drives, portable devices, desktop computers, laptops, photocopiers, fax machines.
- Misdirection of emails and faxes containing confidential information sent to unintended parties.
- Electronic transmission of client confidential information and/or protected health information through secure methods such as encryption or File Transfer Protocol.

III. CONFIDENTIALITY ISSUES CONCERNING CLIENT INFORMATION

In addition to the instructions contained in the specific Administrative/Program policies, the following apply to all DSS staff:

Working with Client Files

DSS Staff are prohibited from accessing, reviewing, or working on case records pertaining to themselves, relatives, friends or acquaintances. If a staff member realizes that a case assigned to him/her involves him/herself, a relative, friend, or acquaintance, the staff member must advise the supervisor immediately, so that the case can be reassigned.

Staff should be aware of the visibility of confidential data or information on their desks, computer screens and throughout their work areas. Confidential information should not be left unattended on staff desks or in other unsecured areas of the office. When staff exit their work areas, they must take every precaution not to leave any confidential information where it may be visible or accessible.

Staff should log-off or lock their computer terminals when they are away from their workstations in order to ensure that no unauthorized person accesses information or performs unauthorized work from their computers.

Staff should avoid taking work home, especially client-related documents, unless it is the standard business practice of the assigned unit or permission is obtained from supervisors. Staff who are authorized to take work home (or e-mail electronic documents to their computer at home) are responsible for ensuring family members or other individuals do not view the documents. Staff should avoid using non-Agency issued equipment, personal email accounts and/or cloud based computing services to access confidential work related materials. Staff should avoid printing hard copies of documents from their home computers, and remain mindful of confidentiality issues at all times when taking work from the office.

HIPAA Rules

Under the federal Health Insurance Portability and Accountability Act (HIPPA) regulations, the Agency and its employees must ensure the privacy and security of all protected health information created, maintained, received or transmitted by the Agency. The term "protected health information" means information which (1) is created or received by HRA/DSS in its role as a as administrator of the New York State Medicaid program.; (2) relates to the health condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and (3) identifies the individual or provides a reasonable basis to believe it can be used to identify an individual. In general, an employee may not use or disclose protected health information pertaining to a client of H R A / DSS except as permitted or required by HIPAA. For more information about HIPAA requirements and restrictions, please see the HRA HIPAA Privacy Policy and Forms Manual, available on HRA eDocs.

Releasing or Disclosing Information Concerning Clients

New York State laws authorize the dissemination of certain confidential information to appropriate parties for specified purposes. Additionally, certain information may be shared with states and agencies that provide similar assistance, in order to prevent duplication and fraud. To ensure clients are receiving appropriate services for which they legally qualify, the Agency may ask other people to confirm the information a client has already submitted to the Agency.

However, the authority to disclose confidential information in specific instances is limited to staff who are designated to handle this function as part of their job responsibilities. Those program areas which routinely have access to client information, including the Family Independence Administration, (FIA), the Medical Insurance and Community Services Administration (MICSA), the Home Care Services Program, the Office of Domestic Violence and Emergency Intervention Services (ODVEIS), the HIV/AIDS Services Administration (HASA), the Investigation, Revenue and Enforcement Administration (IREA), the IDNYC Program, Customized Assistance Services (CAS) and the Department of Homeless Services (DHS), will address confidentiality measures and the disclosure of information specific to their programs in their particular procedures.

Staff Communications

Staff members are prohibited from discussing clients and/or their cases in the presence of others not involved in the cases, and should be especially careful in public areas including elevators, restrooms and waiting areas.

Employees should not discuss any confidential matter with anyone either in person or on the telephone unless the employee is acting in conjunction with his/her job requirements or is specifically authorized by his/her supervisor. Moreover, discussions involving confidential information should be held in as private an area as possible, and in a volume so only those authorized to participate in the conversation can hear what is being discussed. If an employee has any question as to whether an individual is entitled to information, supervisory staff should be consulted before the information is disclosed.

DSS locations shall post signs to remind employees that information acquired during the course of work is not to be shared with other persons unless specifically authorized in writing or by their supervisor. The signs will also explain that disclosure of confidential information to unauthorized persons violates the law and DSS policy.

IV. CONFIDENTIALITY CONCERNS WHEN DEALING WITH OUTSIDE REQUESTS FOR INFORMATION

Disclosing Client Information

Staff members who receive requests for confidential documents and information from applicants, recipients, relatives, law enforcement agencies, governmental agencies, or other entities must be cautioned that the disclosure by this Agency of confidential documents and information is subject both to legal restrictions and to Agency policies regarding the release of such information. Staff should review the email directive from Commissioner Steven Banks, dated March 3, 2017, regarding Confidentiality of Client Information.

In general, DSS's policy prohibits staff from disclosing confidential information to anyone outside the Agency, or to any DSS employee whose duties do not require such disclosure, without a valid consent and/or authorization from the client. Any questions about the validity of written consents and/or authorizations or the disclosure of confidential client information in the absence of valid consent shall be directed to the DSS Chief Data Privacy Officer.

Staff members are prohibited from disclosing on social media client information and other types of confidential and sensitive Agency information. Staff should refer to Informational No. 1-02-13, dated July 10, 2013 for additional information on employee use of social media.

Any DSS employee who is uncertain about whether or not documents or information are confidential should seek guidance from the DSS Chief Data Privacy Officer in the Office of Legal Affairs. Additionally, any DSS employee who is uncertain whether or not it is in the scope of another DSS employee's responsibilities to have access to certain confidential information should seek assistance from his or her supervisor before disclosing the information.

Disclosing Staff Information

General information including staff names, titles, office addresses, and office telephone numbers may be disclosed. Other information regarding staff may not be shared. However, in some instances when sharing such staff information might also affect client information, the staff information should not be shared. For example, the location of DHS shelters and facilities housing survivors of domestic violence or HASA clients should never be disclosed.

Staff members who are unsure about disclosing information to a caller should consult with their supervisor or refer the caller to the DSS Chief Data Privacy Officer or the Agency FOIL Officer. Staff members who have a reason to question the motive of the caller's request for the information should refer to the Commissioner's March 3, 2017 email directive regarding requests for confidential information, and should discuss the call with their supervisor prior to providing the caller with any information. Staff members who have specific reasons for not wanting their information disclosed should inform their supervisor in advance.

Requests for Records

Personnel who have the responsibility for handling requests from outside offices should adhere to the following procedures:

Requests from a client or his or her attorney or authorized representative (with an appropriate release form) for the client's case file or concerning a Fair Hearing shall be handled in the following manner:

- Requests for Evidence Packet/Rivera Requests:

Evidence Packets are directed to the Fair Hearing Administration for MICSA, IREA, FIA and HASA in accordance with Policy Bulletin 05-136-OPE.

- Requests for MICSA/HCSP client case files:

Requests for MICSA/HCSP client case records shall be directed to the HIPAA unit within the Office of Program Accountability Support.

- Requests for FIA case files:

Requests for cash assistance and SNAP records shall be made in accordance with 10-64 OPE.

- Requests for DHS case files:

Requests for DHS case files shall be directed to DHS Records Access within the Office of Legal Affairs.

Requests for Information

- Requests from appropriate law enforcement officers for information in a fraud, criminal or fleeing felon investigation, seeking to identify a person who is a recipient of DSS benefits or services should be referred promptly to:

  Bureau of Fraud Investigations
  250 Church St 3rd Floor
  New York, NY 10013
  929-252-2129

- Requests related to an audit from any agency, including the NYC and NYS Comptroller's Offices, should be referred promptly to:

  Bureau of Audit Coordination
  150 Greenwich Street, 41st Floor
  New York, NY 10007
  929-221-7063

- Requests for information received from any member of the press or media should be directed to:

  Office of Communication and Marketing
  150 Greenwich Street, 42nd Floor
  New York, NY 1007
  212-331-6200

- Requests for information related to litigation, service of subpoenas, and legal questions should be referred to:

  Office of Legal Affairs
  150 Greenwich Street, 38th Floor
  New York, NY 1007
  Data Privacy inquiries: 929-221-6535
  Subpoenas: 929-221-6556

  DSS frequently receives routine requests for confidential information from various entities. Routine data requests include requests for information about clients that occur in the normal course of Agency business, which include requests made pursuant to judicial subpoenas, authorizations, research proposals and court orders. All such requests, including any requests made to HRA or DHS providers/vendors are, and should continue to be, processed through the DSS Office of Legal Affairs.

  Non-routine requests for confidential information, including for purposes unrelated to serving the needs of HRA and DHS clients or for purposes outside the scope of official Agency business, should be promptly referred to the DSS General Counsel.

- Constituent requests should be directed to:

  Office of Constituent Services
  150 Greenwich Street 35th Floor
  New York, NY 10007
  212-331-4640

- FOIL requests for public, non-confidential data should be referred to:

  Freedom of Information Law (FOIL) Officer
  150 Greenwich Street 38th Floor
  New York, NY 10007
  929-221-6556
  Email: FOIL@DSS.nyc.gov

- Requests for information from third parties about child support matters should be directed to:

  Office of Child Support Enforcement—Office of the Deputy Commissioner
  150 Greenwich Street, 40th Floor
  New York, NY 10007
  929-221-4587

- Requests for information from a union official should be directed to:

  Office of Labor Relations
  Deputy Commissioner of DSS Labor Relations
  150 Greenwich Street, 31st Floor
  New York, NY 10007
  929-221-5674

- Requests for information from elected officials or their staff, and requests for information from federal, state and other city agency officials should be directed to:

  Office of Communication and Marketing
  Office of Legislative Affairs
  150 Greenwich Street, 42nd Floor
  New York, NY 1007
  212-331-6200

- Requests for Agency historical data or information should be referred to:

  DSS McMillan Library, Office of Evaluation & Research
  150 Greenwich Street 36th Floor
  New York, NY 10007

DSS's Office of Communications and Marketing has been designated as the Agency's principal office of communication with the media and the public. No employee, except an employee designated by that office or by the Commissioner may present himself or herself as expressing the policies or views of the Agency. An employee who receives an inquiry from the media should refer the inquiry to this office.

Any employee who intends to make a statement in his/her personal capacity to the media, a government agency, a private organization or through social media, must make clear that his/her comments are not official, and represent only his/her personal opinion and not the views or policies of DSS or the City of New York. Any such personal statement made to the media, etc. must be made on the employee's non-working time and not through the use of DSS equipment. The content of these communications shall not contain any information deemed confidential. Please refer to Executive Order No. 686, dated October 21, 2003, for further information regarding the Agency's Press Policy.

Confidentiality Protocol for Researchers

DSS receives numerous requests from outside organizations and individuals for assistance with research projects and studies on subjects related to DSS and its clients. Executive Order No. 679, Approval of External Research Requests and Contracted Research Studies, dated April 16, 2002, addresses issues concerning client confidentiality as related to research projects.

V. CONFIDENTIALITY ISSUES CONCERNING THE USE OF E-MAIL

Staff Responsibilities Concerning the Use of E-mail

All e-mail users must take responsibility for the security and integrity of e-mail transmissions Staff must take all reasonable precautions to ensure that unauthorized individuals do not have access to the information on the staff member's e-mail system. Official DSS business should be communicated via Agency issued e-mails and staff should not use personal e-mails for these types of correspondence. These precautions include safeguarding passwords and changing them periodically. Guidelines for staff use of e-mail are contained in DSS E-Mail Policy, Procedure No. 07-06, March 22, 2007.

Staff should be cautious when including confidential information in e-mail correspondence. E-mail records, once opened, become irrevocable. They create an electronic record that NYC authorities may make available to the public pursuant to the Open Records Act. Staff should also be aware that anything that they write in an e-mail message may be forwarded by the recipient/addressee of the e-mail to others, without the sender's control, approval or knowledge. When sending such e-mails, staff should use encryption software and follow the appropriate protocols with respect to sending encrypted e-mails, where appropriate. Social Security numbers should never be included in the subject line of an e-mail. Before sending large electronic files containing confidential information via e-mail, staff should consult with MIS and/or the OLA Chief Data Privacy Officer to determine what is the most appropriate and secure method for such e-mail transmissions.

Staff should maintain their passwords in a secure location known only to them and should not share them with others.

The following is an example of standard disclaimer language that should be placed at the end of an e-mail containing confidential information:

> 'This e-mail communication, and any attachments, may contain confidential and privileged information for the exclusive use of the recipient(s) named above. If you are not an intended recipient, or the employee or agent responsible to deliver it to an intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please notify me immediately by replying to this message and delete this communication from your computer. Thank you."

Remote User Security

To help guard against confidential information being transmitted over the Internet without the knowledge or consent of a remote user, it is recommended that a personal firewall be used on any computer system that will communicate with DSS computer systems. In addition, with assistance from MIS all remote users must install and maintain an up to date anti-virus program approved by DSS.

VI. GUIDELINES FOR REPRODUCING PRINTED CONFIDENTIAL MATERIALS

Staff who photocopy and scan confidential information should adhere to the following guidelines to ensure that they maintain the confidentiality of the documents being reproduced:

- When copying and scanning documents from a client or staff file, staff should take only necessary documents to the copier/scanner. The remainder of the materials should be kept in the file folder and the file folder placed in a secure location.
- The copier/scanner should not be left unattended while the transmittal is in progress.
- Staff should clear or re-set the copy machine memory after each use.
- Paper jams should be taken care of immediately so paper with possible confidential information is not left in the scanner/copier. If the problem cannot be immediately resolved, a supervisor should be notified.
- Unusable copies that contain confidential information should be shredded.

VII. CONFIDENTIALITY GUIDELINES WHEN USING THE FAX MACHINE

When staff members send or receive a fax containing confidential information they should adhere to the following:

- The time/date/origination stamp that appears at the top of each fax sent from a location should not include the name of the RC if it would indicate to recipients the confidential nature of a client's involvement with DSS. The time/date/origination stamp and the fax cover sheet should indicate only that the document has been sent from DSS, and the telephone number of the sending machine or of such business other entity or individual.
- The cover sheet of a fax containing confidential information should clearly indicate that the information is confidential and intended only for the individual to whom the fax is addressed.
- Whenever practicable, prior to transmitting a fax containing confidential information, staff should call the recipient of the fax to make him/her aware that the fax is being sent.
- A fax containing confidential information should be removed from the fax machine promptly.
- The memory function should not be used to send a fax containing confidential information at a later time. If the recipient's fax machine is busy, clear the memory and send the fax at a later time.
- The fax machine should be checked at periodic intervals throughout the day to ensure confidential material is not left at the fax machine.
- All fax documents should be distributed promptly to the appropriate parties.

VIII. CONFIDENTIALITY GUIDELINES FOR DESTROYING CONFIDENTIAL MATERIALS

When it is no longer necessary to retain paper documents that contain confidential information, these documents must be properly destroyed. Staff should not dispose of documents containing confidential information in bulk, in Agency recycling bins, dumpsters, or any other public receptacles. Staff shall place confidential documents ready for destruction in locked shredding bins located at each program site. Procedure 05-03, Destroying Printed DSS Confidential and Non-Confidential Documents (Non-Records) explains the process. This process adheres to the retention schedules that have been established by the Department of Records and Information Services (DORIS).

IX. CONFIDENTIALITY GUIDELINES CONCERNING CONSULTANTS AND TEMPORARY EMPLOYEES

All Consultants (or temporary employees) shall be required to receive training about DSS's confidentiality policy and sign agreements to:

- Adhere to the requirements of this policy, and the confidentiality policies developed in the program/administrative areas in which they are assigned or otherwise perform work.
- Take all measures that are necessary in order to maintain and protect the confidentiality of the information received while performing their job responsibilities.
- Use the information received only for the performance of the duties assigned.
- Upon the request of DSS or upon completion or termination of their services, return to, or destroy, as may be directed by DSS, all copies of any information, in whatever form such information may exist in their possession.

X. CONFIDENTIALITY ISSUES CONCERNING CONTRACTS

All DSS contracts contain clauses addressing the confidentiality of client information. In addition, programmatic contracts contain specific confidentiality provisions. Some examples of contracts with specific confidentiality requirements include domestic violence, HIV and AIDS Services, WeCARE and drug treatment program contracts. Contract documents and related documentation are confidential prior to registration with the Comptroller's Office. Upon registration, the release of contract documents is subject to the Freedom of Information Law (FOIL) procedure. Requests for the release of registered contracts should be forwarded to the FOIL Officer.

Classification: 02 *Effective: Immediately*