Information Privacy

BIENNIAL AGENCY REPORT

## INSTRUCTIONS

The Identifying Information Law requires City agencies to submit comprehensive biennial agency reports related to their collection, retention, and disclosure of identifying information and their privacy protection practices.

To complete the 2024 biennial agency report:

- Review Form 2s (APO Designation of Collection and Disclosures as "Routine") made since the 2022 compliance cycle;
- Review Form 5s (Agency Privacy Officer Approval of Collections and Disclosures on a "Non-Routine" Basis) made since the 2022 compliance cycle;
- Use Forms 2 & 5 to complete Worksheet 1 for all new and existing **collections** between 2022-2024;
- Use Forms 2 & 5 to complete Worksheet 2 for all new and existing **disclosures** between 2022-2024.
- Complete the Biennial Agency Workbook;
- Submit the biennial agency report by **July 31, 2024**.

Submit the biennial agency report to:

- Mayor at MOReports@cityhall.nyc.gov
- City Council Speaker at reports@council.nyc.gov
- Chief Privacy Officer and the Citywide Privacy Protection Committee at oip@oti.nyc.gov
- Department of Records and Information Services (DORIS) online submission portal at https://a860-gpp.nyc.gov

THIS REPORT IS PUBLIC. PREPARERS SHOULD CONSULT AGENCY COUNSEL OR THE CHIEF PRIVACY OFFICER TO ENSURE THE RESPONSES ARE PROVIDED ACCORDING TO APPLICABLE LAW AND CITY POLICY.

**VERSION CONTROL**

| Version | Description of Change | Approver | Date |
|---|---|---|---|
| 4.0 | New design for ease of use and technological enhancements, and miscellaneous clarifying revisions. | Michael Fitzpatrick<br>Chief Privacy Officer, City of New York | April 2024 |
| 3.0 | Updated completion date; miscellaneous clarifying revisions. | Aaron Friedman<br>Principal Senior Counsel<br>Office of Information Privacy | April 2022 |
| 2.0 | Updated completion date; miscellaneous clarifying revisions. | Laura Negrón<br>Chief Privacy Officer, City of New York | April 2020 |
| 1.0 | First Version | Laura Negrón<br>Chief Privacy Officer, City of New York | April 2018 |

*Page Intentionally Blank*

## BIENNIAL AGENCY REPORT
## (Due on or before July 31, 2024)

1. Agency: Department of Social Services

2. APO Contact Details

   a. Name: Lauren Friedland

   b. Title: DSS Chief Data Privacy Officer, Associate General Counsel

   c. Email: friedlandl@dss.nyc.gov

   d. Telephone: (929) 221-6535

## COLLECTIONS

3. How many collections does the agency have to describe?

   22

4. **COLLECTIONS.** Upload worksheet 1.

***- Proceed to the next page -***

5. For all **collections**, select the types of identifying information collected (check all that apply). *See* Citywide Privacy Protection Policies and Protocols § 3.1.

| | |
|---|---|
| ☒ Name<br>☒ Social security number (full or last 4 digits)*<br>☒ Taxpayer ID number (full or last 4 digits)* | **Work-Related Information**<br>☒ Employer information<br>☒ Employment address |
| **Biometric Information**<br>☒ Fingerprints<br>☒ Photographs<br>☒ Palm and handprints*<br>☐ Retina and iris patterns*<br>☐ Facial geometry*<br>☐ Gait or movement patterns*<br>☒ Voiceprints*<br>☐ DNA sequences*<br>☒ Height<br>☒ Weight | **Government Program Information**<br>☒ Any scheduled appointments with any employee, contractor, or subcontractor<br>☒ Any scheduled court appearances<br>☒ Eligibility for or receipt of public assistance or City services<br>☒ Income tax information<br>☒ Motor vehicle information |
| **Contact Information**<br>☒ Current and/or previous home address<br>☒ Email address<br>☒ Phone number | **Law Enforcement Information**<br>☒ Arrest record or criminal conviction<br>☒ Date and/or time of release from custody of ACS, DOCS, or NYPD<br>☒ Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD |
| **Demographic Information**<br>☒ Country of origin<br>☒ Date of birth*<br>☒ Gender identity<br>☒ Languages spoken<br>☒ Marital or partnership status<br>☒ Nationality<br>☒ Race<br>☒ Religion<br>☒ Sexual orientation | **Technology-Related Information**<br>☒ Device identifier including media access control (MAC) address or Internet mobile equipment identity (IMEI)*<br>☒ GPS-based location obtained or derived from a device that can be used to track or locate an individual*<br>☒ Internet protocol (IP) address*<br>☒ Social media account information |
| **Status information**<br>☒ Citizenship or immigration status<br>☒ Employment status<br>☒ Status as a victim of domestic violence or sexual assault<br>☒ Status as crime victim or witness | |
| **Other Types of Identifying Information** (list below):<br>Program, case, and client numerical identifiers; veteran status; ADA-related information; clinical, mental health, and medical treatment information | |
| *Type of identifying information designated by the CPO (*see* CPO Policies & Protocols, §3.1.1). | |

## DISCLOSURES

6. How many disclosures does the agency have to describe?

   22

7. **DISCLOSURES**. Upload worksheet 2.

***- Proceed to the next page -***

8. For all **disclosures**, select the types of identifying information disclosed (check all that apply). *See* Citywide Privacy Protection Policies and Protocols § 3.1.

| | |
|---|---|
| ☒ Name<br>☒ Social security number (full or last 4 digits)*<br>☒ Taxpayer ID number (full or last 4 digits)* | **Work-Related Information**<br>☒ Employer information<br>☒ Employment address |
| **Biometric Information**<br>☒ Fingerprints<br>☒ Photographs<br>☐ Palm and handprints*<br>☐ Retina and iris patterns*<br>☐ Facial geometry*<br>☐ Gait or movement patterns*<br>☒ Voiceprints*<br>☐ DNA sequences*<br>☒ Height<br>☒ Weight | **Government Program Information**<br>☒ Any scheduled appointments with any employee, contractor, or subcontractor<br>☒ Any scheduled court appearances<br>☒ Eligibility for or receipt of public assistance or City services<br>☒ Income tax information<br>☒ Motor vehicle information |
| **Contact Information**<br>☒ Current and/or previous home address<br>☒ Email address<br>☒ Phone number | **Law Enforcement Information**<br>☒ Arrest record or criminal conviction<br>☒ Date and/or time of release from custody of ACS, DOCS, or NYPD<br>☒ Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD |
| **Demographic Information**<br>☒ Country of origin<br>☒ Date of birth*<br>☒ Gender identity<br>☒ Languages spoken<br>☒ Marital or partnership status<br>☒ Nationality<br>☒ Race<br>☒ Religion<br>☒ Sexual orientation | **Technology-Related Information**<br>☒ Device identifier including media access control (MAC) address or Internet mobile equipment identity (IMEI)*<br>☒ GPS-based location obtained or derived from a device that can be used to track or locate an individual*<br>☒ Internet protocol (IP) address*<br>☒ Social media account information |
| **Status information**<br>☒ Citizenship or immigration status<br>☒ Employment status<br>☒ Status as a victim of domestic violence or sexual assault<br>☒ Status as crime victim or witness | |
| **Other Types of Identifying Information** (list below):<br>Program, case, and client numerical identifiers; veteran status; ADA-related information; clinical, mental healt | |
| *Type of identifying information designated by the CPO (*see* CPO Policies & Protocols, §3.1.1). | |

9. Separate from the Citywide Privacy Protection Policies and Protocols, what are the agency's policies regarding requests for disclosures from other City agencies, local public authorities or local public benefit corporations, and third parties? Please **summarize or upload a copy of the policy**. *See N.Y.C. Admin. Code § 23-1205(a)(1)(c)(1)*.

   DSS/HRA/DHS ("Agency") collects, uses, and/or discloses a wide range of client and employee data and information, most of which is regulated by various federal and state laws, regulations, and policy requirements.

10. Which divisions of employees within the agency make disclosures of identifying information following the approval of the privacy officer? *See § N.Y.C Admin. Code § 23-1205(a)(1)(c)(4)*.

    Various divisions within the Agency make disclosures of identifying information pursuant to the Agency's confidentiality policies and procedures. The division or unit responsible for making the disclosure depends on the nature of the request (e.g., who is making the request and the type of information being requested).

11. Which categories of employees within the agency make disclosures of identifying information following the approval of the privacy officer? *See § N.Y.C Admin. Code § 23-1205(a)(1)(c)(4)*.

    Various categories of employees within multiple divisions of the Agency make disclosures of identifying information pursuant to the Agency's confidentiality policies and procedures. The type of employee responsible for making the disclosure depends on the Agency division handling the request, as well as the employee's specific job functions and responsibilities.

12. Do any of the agency's policies address **access** to identifying information by employees, contractors, and subcontractors? *See § N.Y.C. Admin Code § 23-1205(a)(4).*

    ◉ Yes – **GO TO QUESTION 13**

    ○ No – **GO TO QUESTION 16**

13. Do these policies state that **access** to identifying information must be necessary for the employees, contractors, and subcontractors to perform their duties? *See N.Y.C. Admin Code § 23-1205(a)(4).*

    ◉ Yes – **GO TO QUESTION 14**

    ○ No – **GO TO QUESTION 16**

14. Are these policies implemented so that **access** is limited to the greatest extent possible, but also furthers the purpose or mission of the agency?

    ◉ Yes – **GO TO QUESTION 15**

    ○ No – **GO TO QUESTION 16**

15. Describe how **access** is limited to the greatest extent possible while furthering the purpose or mission of the agency.

    In addition to compliance with the cybersecurity and data protection guidance issued by the Office of Cyber Command, the Agency utilizes various administrative, technical, physical, and operational safeguards to limit access to data without hindering the Agency's provision of services.

    For example, requests for access to electronic databases and case management systems are approved only if such access is necessary to carry out assigned job functions. If a request is approved, the requestor's assigned user role imposes access and functional limits (e.g., read-only or otherwise

16. **Summarize or upload** the agency's current policies for handling **proposals for disclosures to other** City agencies, local public authorities, or local public benefit corporations, and third parties. *See N.Y.C Admin Code § 23-1205(a)(1)(c)(2)*.

    See question #9 and attached confidentiality policies and procedures.

17. **Summarize or upload** the agency's current policies regarding the classification of **disclosures** as necessitated by the existence of **exigent circumstances or as routine**. *See N.Y.C Admin Code § 23-1205(a)(1)(c)(3)*.

    The Agency APO classifies a disclosure as "routine" if the disclosure is made during the normal course of Agency business and furthers the Agency's mission. The Agency APO classifies a disclosure as "necessitated by exigent circumstances" if the disclosure was too urgent to wait for APO approval and was also necessary to address an imminent threat to health and safety.

18. Since 2022, has the agency **considered or implemented**, where applicable, policies that minimize the collection, retention, and disclosure of identifying information to the greatest extent possible while furthering the purpose or mission of the agency? *See N.Y.C Admin Code § 23-1205(a)(3)*.

    ◉ Yes – **GO TO QUESTION 19**

    ○ No – **GO TO QUESTION 20**

19. Summarize the policies that the agency has **considered or implemented** regarding data minimization for the collection, retention, and disclosure of identifying information. *See N.Y.C Admin Code § 23-1205(a)(4)*.

    See question #9 and attached policies and procedures.

20. Summarize the agency's use of agreements for any use or disclosure of identifying information. *See N.Y.C Admin Code § 23-1205 (a)(1)(d)*.

    The Agency utilizes agreements for data sharing initiatives involving sensitive identifying information and/or identifying information that is restricted by other laws and regulations—regardless of whether the disclosures involved have been or will be designated as routine.

    For these agreements, the Agency includes the appropriate riders or attachments pursuant to guidance issued by the Chief Privacy Officer. Additionally, the Agency includes OTI's "Attachment SCY" in

21. Since 2022, describe the impact of the Identifying Information Law and any other local, state, or federal laws upon your agency's practices in relation to the collection, retention, and disclosure of identifying information (i.e., if such practices would differ in the absence of these laws). The impact can be positive or negative. *See N.Y.C Admin Code § 23-1205(a)(2)*.

    No significant impact to report.

22. Describe how the current privacy policies and protocols issued by the Chief Privacy Officer, or the guidance issued by the Citywide Privacy Protection Committee affected your agency's practices in relation to the collection, retention, and disclosure of identifying information. The effects can be positive or negative. *See N.Y.C Admin Code § 23-1205(a)(2)*.

    The various APO resources issued by the Chief Privacy Officer and the Office of Information Privacy have enhanced the Agency's ability to draft data sharing / confidentiality / non-disclosure agreements for emergency and special projects on an expedited basis.

    Such policies, protocols, and guidance have also increased and expanded the Agency's compliance and reporting workload.

***- Proceed to the next page -***

NYC OTI
Information Privacy

## APPROVAL SIGNATURE FOR AGENCY REPORT

### PREPARER OF AGENCY REPORT

Name: Jessica Pulitzer

Title: Senior Attorney

Email: pulitzerj@dss.nyc.gov

Phone: (929) 221-6656

### ELECTRONIC SIGNATURE OF AGENCY HEAD OR DESIGNEE REQUIRED BELOW

Name: Molly Park

Title: Commissioner

Email: parkmo@dss.nyc.gov

Phone: 929-221-7315

Signature: Molly Park
Molly Park (Jul 26, 2024 15:57 EDT)

Date: 07/26/2024

**Describe the following types of collections.** *Note, you may have multiple collections of the same type.*

| COLLECTIONS | | | | |
|---|---|---|---|---|
| | *Type of Collection* | *Describe the Specific Activity* | *Classification* | *Describe the agency purpose or mission served by this Collection.* |
| 1 | Legal Matters or Proceeding | Collect identifying information while performing work related to appearing for, representing, or responding to legal matters and proceedings involving adjudicative and administrative bodies, arbitrators, the Law Department or other counsel, and other persons or entities with an interest in the agency's legal matter or proceeding. | Pre-approved as routine | Represent the agency in legal proceedings, including but not limited to litigation and administrative proceedings. |
| 2 | Human Resources and other Personnel Matters | Collect identifying information while performing human resources and other personnel-related activities, including processing new hires, retiree and benefits processing, payroll processing, equal employment opportunity matters, training, occupational health and safety matters, and professional development. | Pre-approved as routine | To support the agency's workforce and ensure day-to-day human resources and personnel needs are met. |
| 3 | Law Enforcement | Collect identifying information, subject to applicable law, from local, state, or federal law | Pre-approved as routine | To help ensure the agency's compliance with federal, state, and local laws and rules regarding |

| | | | | |
|---|---|---|---|---|
| | | enforcement authorities for purposes of law enforcement activities, which may include the investigation, prosecution, or enforcement of a law, regulation, rule, or order. | | law enforcement inquiries, investigations, and related matters. |
| 4 | Compliance | Collect identifying information, subject to applicable law, to comply with regulations, rules, guidelines, conditions, and rules related to program funding. | Pre-approved as routine | To ensure agency's compliance with various federal, state, and local laws and rules governing agency programs and services, as well as rules regarding client privacy, confidentiality, and data security. |
| 5 | Audit | Collect identifying information from federal, state, or local auditors, or other entities authorized to perform audits, in compliance with applicable laws or regulations. | Pre-approved as routine | To ensure agency's compliance with federal, state, and local laws and rules related to cooperating in audits and oversight activities conducted by entities authorized to oversee and audit the agency's provision of services. |
| 6 | Procurement | Collect identifying information from contractors, experts, or consultants to bid and negotiate procurements and to enter into agreements with the agency so that such entities or persons may carry out their roles and responsibilities under such agreements. | Pre-approved as routine | To support agency's ability to procure, monitor, and support the various roles and responsibilities of agency vendors, contractors, subcontractors, consultants, and experts. |

| | | | | |
|---|---|---|---|---|
| 7 | Public Safety and Health | Collect identifying information as needed from appropriate federal, state, and local agencies or personnel as it relates to citywide emergency services and preventing and combating public health and safety threats. | Pre-approved as routine | To ensure agency employees and clients can work and seek out services and benefits in a healthy and safe environment. |
| 8 | Prevention of Fraud, Waste, Abuse | Collect identifying information for the purpose of detecting, preventing, or recovering from fraud, waste, abuse, or improper payments that may have occurred in agency programs regulated by federal, state, and local government. | Pre-approved as routine | To ensure agency's compliance with federal, state, and local laws and rules to prevent, identify, and address fraud, abuse, and waste. |
| 9 | Client or Customer Service | Collect identifying information to provide service or support to agency clients. | Pre-approved as routine | To support agency's responsibility to respond to client requests and support client needs. |
| 10 | Response to a Request or Demand | Collect identifying information to respond to FOIL requests and inquiries for information submitted by elected officials, legal representatives and counsel, and other third parties and entities seeking general and identifying information. Prior to responding to such requests, appropriate agency personnel determine whether collecting/disclosing requested | Pre-approved as routine | To support agency's responsibility to respond to third-party requests for information that are in furtherance of the agency's mission. |

| | | | | |
|---|---|---|---|---|
| | | information is permissible under applicable law, regulation, and/or rule. | | |
| 11 | Incident Management | Collect identifying information where it has been determined or suspected that the confidentiality of identifying information has been compromised, and such collection is either required by law or is reasonably necessary to assist in efforts to prevent, minimize, or remedy potential or actual harm. | Pre-approved as routine | To support and facilitate agency's ability to respond to data security incidents and breaches, including but not limited to incident response, client notification, implementation and oversight of corrective action plans, among other activities. |
| 12 | Technology | Collect identifying information in the performance of information technology-related functions, including hosting, database administration and management, helpdesk, asset management, and other technical services related to electronic infrastructure and data. | Pre-approved as routine | To support agency's day-to-day and special technology needs and maintain and enhance technological processes and infrastructures. |
| 13 | Social Services | Collect identifying information to support the work necessary for the provision of social services, benefits, and programs, including but not limited to adjudicating | Pre-approved as routine | To support the agency's mission to serve New Yorkers in need through the administration of a wide range of benefits and services including but not limited to food and cash assistance, |

| | | | | |
|---|---|---|---|---|
| | | eligibility, determining appropriate service or benefit amount, and related activities to ensure the provision of social services to which individuals are legally entitled. | | emergency and ongoing rental and utility assistance, job placement and trainings, public health insurance, childcare, adult protective services, domestic violence shelter, and homelessness. |
| 14 | Strategic Initiatives | Collect identifying information as part of new or non-routine initiatives, including but not limited to public engagement efforts, new or ongoing mayoral initiatives and projects involving multiple agencies on a citywide priority. | Approved by the APO on a case-by-case basis | To support agency's ability to collaborate with other city agencies on mayoral projects and other unique citywide initiatives. |
| 15 | Records Management | Collect identifying information for records management, archiving, and preservation pursuant to applicable federal, state, and local laws and regulations. | Pre-approved as routine | To facilitate agency's ability to comply with federal, state, and local laws and rules governing record management and retention. |
| 16 | Finance | Collect identifying information for invoices, checks, budgets, financial reports, and other financial information related to fiscal operations. | Pre-approved as routine | To support agency's fiscal operations. |
| 17 | Office Administration | Collect identifying information for day-to-day administrative functions, including but not limited to filing, personnel- | Pre-approved as routine | To support agency's ability to function and maintain day-to-day office administration. |

| | | | | |
|---|---|---|---|---|
| | | related work, scheduling appointments, billing, and maintaining records. | | |
| 18 | Research | Collect identifying information for research projects (including research collaborations with external partners) to conduct survey, interviews, focus groups, and other research activities that help inform program planning, resource management, agency policies, practices, and public outreach. | Approved by the APO on a case-by-case basis | To support agency's efforts to maintain, enhance, and improve services to clients on an individual and agency-wide level. |
| 19 | Education | Collect identifying information related to academic, education, and student information, including but not limited to childcare and educational services. | Pre-approved as routine | To support agency's service delivery and administration of services and benefits related to childcare, education, and related needs. |
| 20 | Housing | Collect identifying information for housing-related services, including eligibility determinations for temporary or emergency shelter, affordable housing, rental assistance, and eviction protection and prevention services. | Pre-approved as routine | To support the agency's provision of housing-related support services, benefits, and programs. |
| 21 | Environment | Collect identifying information to manage environmental | Pre-approved as routine | To support agency's ability to maintain and enhance facilities, |

| | | | | |
|---|---|---|---|---|
| | | initiatives or sustainability projects, such as capital construction and site enhancement. | | buildings, and workspaces, including site enhancements and capital construction. |
| 22 | Utilities & Infrastructure | Collect identifying information for the purposes of creating, developing, testing, enhancing, and maintaining the physical and technical infrastructure of the agency facilities, buildings, and workspaces. | Pre-approved as routine | To facilitate agency's ability to maintain and enhance physical and technical infrastructure of agency facilities, buildings, and workspaces. |

***Please add additional rows, if needed***

**Describe the following types of disclosures.** *Note, you may have multiple disclosures of the same type.*

| DISCLOSURES | | | | | |
|---|---|---|---|---|---|
| | *Type of Disclosure* | *Describe the Specific Activity* | *Classification* | *Describe the agency purpose or mission served by this Disclosure.* | *Was this disclosure made pursuant to an external request?* |
| 1 | Legal Matters or Proceeding | Disclose identifying information while performing work related to appearing for, representing, or responding to legal matters and proceedings involving adjudicative and administrative bodies, arbitrators, the Law Department or other counsel, and other persons or entities involved in the agency's legal matter or proceeding. | Pre-approved as routine | Represent the agency in legal proceedings and adverse litigation or administrative proceedings. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 2 | Human Resources and other Personnel Matters | Disclose identifying information while performing human resources and other personnel matters, including new hire processing, retiree and benefits processing, | Pre-approved as routine | To support the agency's workforce and ensure day-to-day human resources and personnel needs are met. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| | | payroll processing, equal employment opportunity matters, training, occupational health and safety matters, and professional development. | | | |
| 3 | Law Enforcement | Disclose identifying information, subject to applicable law, to local, state, or federal law enforcement authorities for purposes of law enforcement activities, which may include the investigation, prosecution, or enforcement of a law, regulation, rule, or order. | Approved by the APO on a case-by-case basis | To help ensure the agency's compliance with federal, state, and local laws and rules regarding law enforcement inquiries, investigations, and related matters. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 4 | Compliance | Disclose identifying information, subject to applicable law, to oversight entities and agencies to comply with regulations, rules, guidelines, and conditions and rules related to program funding. | Pre-approved as routine | To ensure agency's compliance with various federal, state, and local laws and rules governing agency programs and services, as well as rules regarding client privacy, confidentiality, and data security. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Audit | Disclose identifying information to federal, state, or local auditors, or other entities authorized to perform audits, in compliance with applicable laws or regulations. | Pre-approved as routine | To ensure agency's compliance with federal, state, and local laws and rules related to cooperating in audits and oversight activities by entities authorized to engage in agency oversight. | Yes |
| 6 | Procurement | Disclose identifying information to contractors, subcontractors, experts, or consultants to bid and negotiate procurements and to enter into agreements with the agency so that such entities or persons may carry out their roles and responsibilities under such agreements. | Pre-approved as routine | To support agency's ability to procure, monitor, and support the various roles and responsibilities of agency vendors, contractors, subcontractors, consultants, and experts. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 7 | Public Safety and Health | Disclose identifying information as needed to appropriate federal, state, and local agencies or personnel as it relates to citywide emergency services and preventing | Pre-approved as routine | To ensure agency employees and clients can work and seek out services and benefits in a healthy and safe environment. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| | | and combating public health and safety threats | | | |
| 8 | Prevention of Fraud, Waste, Abuse | Disclose identifying information for the purpose of detecting, preventing, or recovering from fraud, waste, abuse, or improper payments that may have occurred in agency programs regulated by federal, state, and local government. | Pre-approved as routine | To ensure agency's compliance with federal, state, and local laws and rules to identify, address, and prevent (if possible) fraud, abuse, waste, and other bad acts. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 9 | Client or Customer Service | Disclose identifying information to agency clients, authorized representatives and other appropriate third parties for purposes related to serving clients and responding to requests and complaints. | Pre-approved as routine | To support agency's responsibility to respond to client requests and support client needs. | Yes |
| 10 | Response to a Request or Demand | Disclose identifying information to respond to inquiries for information submitted under FOIL, as well as requests for information by elected officials, legal representatives, legal | Pre-approved as routine by the APOs of two or more agencies | To support agency's responsibility to respond to third-party requests for information that are in furtherance of the agency's mission. | Yes |

| | | | | | |
|---|---|---|---|---|---|
| | | counsel, and other third parties and entities seeking general and identifying information. Prior to responding to such requests, appropriate agency personnel determine whether disclosing requested information is permissible under applicable law, regulation, and/or rule. | | | |
| 11 | Incident Management | Disclose identifying information to appropriate agencies, entities, or persons where it has been determined or suspected that the confidentiality of identifying information has been compromised, and that such disclosure is either required by law or is reasonably necessary to assist in efforts to prevent, minimize, or remedy potential or actual harm. | Approved by the APO on a case-by-case basis | To support and facilitate agency's ability to respond to data security incidents and breaches, including but not limited to incident response, client notification, implementation, and oversight of corrective action plans, among other activities. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| 12 | Technology | Disclose identifying information in the performance of information technology-related functions, including hosting, database administration and management, helpdesk, asset management, and other technical services related to electronic infrastructure and data. | Pre-approved as routine | To support agency's day-to-day and special technology needs and maintain and enhance technological processes and infrastructures. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 13 | Social Services | Disclose identifying information to facilitate the provision of social services, benefits, and programs, including but not limited to adjudicating eligibility, determining appropriate service or benefit amount, and related activities to ensuring provision of social services to which individuals are legally entitled. | Pre-approved as routine | To support the agency's mission to serve the New Yorkers in need through the administration of services, benefits, and programs that help clients address and overcome food insecurity, financial distress, homelessness, and eviction, along with addressing other needs, including but not limited to medical and mental health needs. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 14 | Strategic Initiatives | Disclose identifying information as part of | Approved by the APO on a case-by-case basis | To support agency's ability to collaborate with | Disclosures made pursuant to external |

| | | | | | |
|---|---|---|---|---|---|
| | | new or non-routine initiatives, including but not limited to public engagement efforts, new or ongoing mayoral initiatives and projects involving multiple agencies on a citywide priority. | | other city agencies on mayoral projects and other unique citywide initiatives. | requests and based on agency's internal needs. |
| 15 | Records Management | Disclose identifying information for records management, archiving, and records preservation pursuant to applicable federal, state, and local laws and regulations. | Pre-approved as routine | To facilitate agency's ability to comply with federal, state, and local laws and rules governing record management and retention. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 16 | Finance | Disclose identifying information for invoices, checks, budgets, financial reports, and other financial information related to fiscal operations. | Pre-approved as routine | To support agency's fiscal operations. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 17 | Office Administration | Disclose identifying information for day-to-day administrative functions, including but not limited to filing, personnel-related work, scheduling | Pre-approved as routine | To support agency's ability to function and maintain day-to-day office administration. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| | | appointments, billing, and maintaining records. | | | |
| 18 | Research | Disclose identifying information for research projects (including research collaborations with external partners) to conduct surveys, interviews, focus groups, and other research activities that help inform program planning, resource management, agency policies, practices, and public outreach. | Approved by the APO on a case-by-case basis | To support agency's efforts to maintain, enhance, and improve services to clients on an individual and agency-wide level. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 19 | Education | Disclose identifying information related to academic, education, and student information, including but not limited to childcare and educational services. | Pre-approved as routine | To support agency's service delivery and administration of services and benefits related to childcare, education, and related needs. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 20 | Housing | Disclose identifying information for housing-related services, including eligibility determinations for temporary or emergency shelter, affordable housing, rental | Pre-approved as routine | To support the agency's provision of housing-related support services, benefits, and programs. | Disclosures made pursuant to external requests and based on agency's internal needs. |

| | | | | | |
|---|---|---|---|---|---|
| | | assistance, and eviction protection and prevention services. | | | |
| 21 | Environment | Disclose identifying information to manage environmental initiatives or sustainability projects, such as capital construction and site enhancement. | Pre-approved as routine | To support agency's ability to maintain and enhance facilities, buildings, and workspaces, including site enhancements and capital construction. | Disclosures made pursuant to external requests and based on agency's internal needs. |
| 22 | Utilities & Infrastructure | Disclose identifying information for the purposes of creating, developing, testing, enhancing, and maintaining the physical and technical infrastructure of the agency facilities, buildings, and workspaces. | Pre-approved as routine | To facilitate agency's ability to maintain and enhance physical and technical infrastructure of agency facilities, buildings, and workspaces. | Disclosures made pursuant to external requests and based on agency's internal needs. |

***Please add additional rows, if needed***

For each **disclosure**, select the type of entity **and** provide the name of the entity that received the identifying information.

| | *Type of Entity* | *Name of Entity* |
|---|---|---|
| 1 | Each disclosure type listed above involves one of more of the following types of entities: federal agencies, state agencies, city agencies, educational institutions, financial institutions, research institutions, media outlets, law firms, consulting firms, accounting firms, healthcare organizations, transportation carriers, private sector companies, and nonprofits. | Various. |

***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*

**DSS Policy Bulletin #2022-001**
***Date:*** February 8, 2022

**DISTRIBUTION: *ALL STAFF, CONTRACTORS AND SUBCONTRACTOS***

# CONFIDENTIALITY AND DATA PROTECTION POLICY FOR DSS-HRA-DHS CONTRACTORS AND SUBCONTRACTORS

## Table of Contents



## I. INTRODUCTION

This confidentiality policy is directed to all New York City Department of Social Services (DSS), Human Resources Administration (HRA) and Department of Homeless Services (DHS) contractors, vendors, contracted providers and subcontractors, hereinafter referred to as “contractors.” The purpose of this policy is to inform all contractors of their obligations and responsibilities pertaining to the collection, retention and disclosure of confidential information obtained by or on behalf of the City of New York, as well as information provided by the City to contractors. These requirements apply to all forms of collection and disclosure, including but not limited to paper and electronic forms and oral communications, and to all devices, applications, systems, and files which contain confidential information.

Contractors should be aware that DSS-HRA-DHS program areas may also have additional confidentiality policies and procedures which are applicable to contractors and which may be more specifically tailored to the needs of each program area. The purpose of this policy is to supplement any existing confidentiality policies or procedures that apply to contractors and it should be noted that this policy does not replace or render any existing policies or agreements obsolete. Contractors should be aware of their responsibilities and obligations under all DSS-HRA-DHS confidentiality policies and procedures. Contractors should also ensure that all of their employees, subcontractors, agents, and volunteers comply with the information security standards and requirements set forth by the New York City Department of Information Technology and Telecommunications and the New York City Cyber Command and the Citywide Privacy Protection Policies and Protocols established by the New York City Chief Privacy Officer.

In accordance with this policy, Contractors agree to use and ensure the use of appropriate safeguards to prevent misuse or unauthorized disclosure of the data. Contractors are required to implement administrative, physical, and technical safeguards consistent with industry standards that reasonably and appropriately protect and secure the confidentiality, integrity, and availability of any electronic or hard copy individually identifiable information that is created, received, maintained, uploaded, exchanged or transmitted.

## II. OVERVIEW

The collection, retention, use and disclosure of confidential information should be consistent with and limited to the terms provided under the City contracts, and in accordance with all applicable local, state, and federal statutes and regulations and any attached Identifying Information Law Riders. At no time during or after the term of the contract, shall contractors use Agency confidential information for the benefit of itself or any third party in any manner inconsistent with the terms and conditions of any contract or data sharing agreement.

## III. OWNERSHIP OF CONFIDENTIAL DATA

In general, confidential information provided to any contractor by the Agency for purposes of the performance of services on behalf of the Agency shall remain the exclusive property of New York City, with the exception of confidential information obtained by contractors from clients in the course of providing contracted legal services to such clients. Unless otherwise specified under the terms of their contracts, confidential information provided by the Agency to contractors and maintained in connection with contractor services are owned by the City and no right, title, or interest in any material developed therefrom is transferred to the contractor.

## IV. DEFINITIONS

**A**. "Record" means any paper or electronic file or document which contains Confidential Information.

**B**. “Confidential information” means 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.

**C**. “Employee” means any person employed by a contractor or subcontractor whether employed full time, part time or on a temporary or seasonal basis, as well as any officers, representatives, consultants, researchers, agents or any other person or entity given access to Agency confidential or identifying information.

**D**. “Identifying information” means any information obtained by or on behalf of the City that may be used on its own, or with other information, to identify or locate an individual. Note that information from various or seemingly unrelated sources that may not have been identifiable or specific on its own may rise to the level of “identifying” when combined with other available information. Examples of identifying information include: name, full or partial social security number, photographs, current or previous home address, gender identity, citizenship or immigration status, employment status, eligibility for or receipt of public assistance, scheduled appointment times, location and internet protocol address.

**E**. “Identifying Information Law” shall refer to the New York City Local Laws 245 and 247 which set forth new requirements concerning the collection, retention, and disclosure of identifying information by City agencies and health and human services contractors, technology services contracts and certain types of outreach contracts. The Citywide Privacy Officer has the authority to expand the applicability of the Identifying Information Law to other types of contractors over time.

**F**. “Health and Human services” means any services provided to third parties, including social services such as day care, foster care, home care, homeless assistance, housing and shelter assistance, preventive services, youth services, and senior centers; health or medical services including those provided by health maintenance organizations; legal services; employment assistance services, vocational and educational programs; and recreation programs.

**G**. “Technology Services Contracts” means contracts and subcontracts for technology services involving sensitive identifying information collected by the contractor or subcontractor on behalf of the City. Such contractors and subcontractors collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information, even if access to sensitive information is not the express purpose of the contract.

**H**. “Outreach services” means certain contracts and subcontracts for outreach services services involving identifying information. These are contracts or subcontracts where the contractor or subcontractor collects, uses, or discloses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events through any means. This designation does not include agency contracts with a vendor to perform outreach services to the agency’s own clients.

**I**. “Data security incident” refers to the suspected or actual disclosure of any confidential information to a third party without authorization, whether the disclosure is intentional or accidental, or when confidential information is used, acquired, or accessed for improper purposes.

## V. ROUTINE COLLECTIONS AND DISCLOSURES

The Identifying Information Law which applies to health and human services contractors, technology services contracts and certain outreach services contracts required each City agency to appoint an Agency Privacy Officer charged with assessing compliance and designating certain types of collections and disclosures of identifying information as “routine”. Disclosures for functions or purposes designated as routine generally do not require further approval from the DSS Agency Privacy Officer (APO) prior to the disclosure of identifying information. The DSS APO has designated a number of routine collections and disclosures, for example, responding to subpoenas, court orders, audits, and program eligibility determinations.

It is the Contractor’s responsibility to review the APO’s routine designations to ensure that all collections and disclosures of identifying information are made in accordance with the APO’s prior approval. Please note that the APO’s designations were made with current Agency and contractor operations in mind. If legal review was required for a particular disclosure prior to enactment of the law, such review is still required.

Except under emergency circumstances, Contractors must seek approval from the APO prior to any collection, retention, use or disclosure of identifying information for any purpose that has not been designated as routine or is outside of the scope of their respective agreements. Collections or disclosures of any identifying information that have not been designated as routine must be approved by the DSS APO on a case-by-case basis. If a collection or disclosure is made under emergency circumstances, this should be reported to the DSS APO using the contact information at the bottom of this communication.

Additionally, contractors must fully cooperate with audits and investigations to the extent permitted by law when formal requests for confidential information are made for these purposes. If confidential information is sought from Contractors by subpoena, court order or FOIL request, Contractors shall consult with the DSS Office Legal Affairs prior to the disclosure and unless legally prohibited from doing so, provide reasonable written notice and a copy of the request to DSS Office of Legal Affairs. No Confidential Information may be disclosed without authorization from the DSS Office of Legal Affairs unless such disclosure is required by law.

## VI. DATA INVOLVING HEIGHTENED EXERCISE OF CARE

Contractors should be aware that there should be a heightened exercise of care when collecting, using, and disclosing certain types of highly sensitive confidential data as required under applicable local, state, and federal statutes and regulations. There are certain types of confidential information that would pose a higher risk of harm to clients if improperly disclosed. Examples of such data include but are not limited to individually identifiable protected health information under the Health Insurance Portability and Accountability Act (HIPAA), HIV-AIDS status information under Article 27-F of the NYS Public Health Law, Domestic Violence status and Domestic Violence address information under VAWA 34 USC § 12291(b)(2) and NY Social Services Law § 459-h, drug and alcohol use information under 42 U.S.C.§290dd-2 and mental health status information under the NYS Mental Hygiene Law §33.13. Contractors are responsible for complying with all applicable local, state and federal law that govern the use and disclosure of confidential information.

Contractors whose services require receiving and maintaining Protected Health Information from the HRA covered entity which administers the Medicaid program must also enter into business associate agreements with the covered entity, in addition to their underlying agreements. The HIPAA Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associates that the business associates will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. Please note that business associates are required to report security and privacy breaches to the covered entity under 45 CFR § 164.410.

## VII. CIVIL LIABILITY, CRIMINAL PROSECUTION AND CONTRACT TERMINATION

Any unauthorized access to, or disclosure of confidential information may result in civil liability, monetary civil penalties, a private lawsuit, or a criminal prosecution. Contractors should not access any active, closed or archived case record, including, but not limited to the record of a relative, acquaintance, neighbor, friend, partner, co-worker, themselves or any other individual, except in the performance of official job duties and for authorized purposes, utilizing approved processes for such access and in accordance with federal and state laws, rules, regulations, policies and agreements. Please be advised that a contract may be terminated as a result of an incident involving the unauthorized disclosure of HRA-DSS-DHS data.

## VIII. DATA SECURITY INCIDENT AND REPORTING REQUIREMENTS

Data security incidents have the potential to cause harm to clients, including but not limited to financial, physical, emotional, and reputational harm. There is also a risk of reputational harm and financial liability to DSS-HRA-DHS and the City. It is important for Contractors to be aware of these risks and also be able to recognize and identify a data security incident. Examples of data security incidents may include but are not limited to:

- unauthorized access to identifying information
- disclosure of identifying information to unauthorized third parties
- loss (even temporary) or inadvertent disclosure or release of identifying information except during exigent (emergency) circumstances, collecting, retaining, or disclosing identifying information without prior routine or case-by-case approval of the Agency Privacy Officer.
- Loss, theft or improper disposal of equipment, including work-issued cell phones, CDs, thumb drives, portable devices, desktop computers, laptops, photocopiers, fax machines.
- Loss, theft, or improper disposal of hard copy documents that contain confidential and personally identifiable information.
- Misdirection of emails, mails/correspondence and faxes containing confidential information that are sent to unintended parties.
- Suspected or actual instances of computer hacking, ransomware, and phishing attacks.
  Examples of phishing attacks include situations where threat actors disguise themselves as a trusted entity to dupe individuals into opening suspicious emails or trick them into clicking on a malicious link in an attempt to gain privileged access, steal user data such as login credentials and financial information and/or install malware which can result in the freezing of the system.
- Release of confidential information in response to a fraudulent email or telephone call.
- Disclosure of confidential information to the internet or any social media sites.
- Unauthorized copying of confidential Agency information to personal electronic devices, such as routers, thumb drives, and other non-secure environments without prior authorization from DSS-HRA-DHS. etc.

Contractors shall fully cooperate with DSS-HRA-DHS regarding any investigations related to the unauthorized disclosure of confidential data.

Contractors shall immediately report to the Agency the discovery of any unauthorized use or disclosure of confidential information directly to security@dss.nyc.gov and cooperate with additional information requests.

*Effective Immediately*