Mayor's Office of Information Privacy

LAURA NEGRÓN
CHIEF PRIVACY OFFICER

Citywide Privacy Protection Policies and Protocols

January 28, 2019

Page Intentionally Blank

Mayor's Office of Information Privacy

VERSION CONTROL

Version	Description of Change	Approver	Date
1.0	First Version	Laura Negrón Chief Privacy Officer, City of New York	1/28/2019

Mayor's Office of Information Privacy

Page Intentionally Blank

Mayor's Office of Information Privacy

LAURA NEGRÓN
CHIEF PRIVACY OFFICER

Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer, City of New York

Table of Contents

Mayor's Office of Information Privacy

Page Intentionally Blank

Mayor's Office of Information Privacy

LAURA NEGRÓN
CHIEF PRIVACY OFFICER

Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer, City of New York

1.0 Introduction

1.1 Purpose and Scope

This document sets forth the citywide privacy protection policies and protocols of the Chief Privacy Officer of the City of New York ("Policy") governing the collection, retention, and disclosure of identifying information by City agencies and certain City contractors and subcontractors, in accordance with the requirements of subdivision (h) of section 8 of the New York City Charter ("Charter") and sections 23-1201 through 23-1205 of the New York City Administrative Code ("Admin. Code") (together, the "Identifying Information Law").[1]

1.2 Authority

This Policy is issued pursuant to the powers and duties accorded to the Chief Privacy Officer under Charter § 8(h)(1), and is informed by both the requirements set forth in Admin. Code § 23-1203 and the recommendations of the Citywide Privacy Protection Committee, dated October 26, 2018.[2]

1.3 Applicability

This policy applies to all City agencies except those exempt from the requirements of the Identifying Information Law (refer to **Appendix A** for a list of exempt City entities). Additionally, City agency contractors and subcontractors with contracts or subcontracts for the provision of human services[3] and other services designated by the Chief Privacy Officer ("covered contractors and subcontractors") must comply with this Policy.[4]

The agency privacy officer[5] has key responsibilities for implementing the requirements of the Identifying Information Law and facilitating agency compliance with this Policy. Compliance at the agency level is, however, ultimately the responsibility of the agency head. The agency privacy officer should seek guidance from the Chief Privacy Officer as necessary to facilitate agency compliance with the Identifying Information Law and this Policy.

1.4 Modification

This Policy is a living document and may be amended from time to time by the Chief Privacy Officer to address additional requirements and privacy protection best practices for City agencies and covered contractors and subcontractors

[1] In December 2017, the New York City Council enacted Local Laws 245 and 247, which set forth new requirements concerning the collection, retention and disclosure of "identifying information" by City agencies and certain covered contractors and subcontractors. The Law went into effect on June 15, 2018.
[2] The Citywide Privacy Protection Committee is the committee established in accordance with the requirements of Admin. Code § 23-1204.
[3] "Human services" has the mearing set forth in Admin. Code § 6-129(c).
[4] Refer to **Section 6.0** of this Policy on Contracts.
[5] The Identifying Information Law requires each agency head to designate an individual to act as its privacy officer. See Admin. Code § 23-1201. Refer to **Section 4.0** of this Policy for more information about the roles and responsibilities of the agency privacy officer.

relating to the collection, retention, and disclosure of identifying information. Any modifications to this Policy will be made by the Chief Privacy Officer with notification and distribution of the amendment to appropriate agency personnel.

1.5 Relationship to Other Relevant City and Agency Policies

1.5.1 Executive Order No. 34 of 2018

Executive Order No. 34 of 2018, which establishes the Mayor's Office of Information Privacy and the Citywide Privacy Protection Committee within the Office of the Mayor, recognizes the City's commitment to improving the coordination of City resources and services across agencies to ensure that residents from all backgrounds and communities can thrive and prosper and receive the right services at the right time, as reflected in OneNYC,[6] and the need for robust information privacy and security protections to facilitate access by all New Yorkers to important City services and resources. Consistent with Executive Order 34 and the goals of OneNYC, this Policy sets forth requirements and guidance on privacy and security protection in a manner so as to guide City agencies in responsibly sharing data in furtherance of important City and cross-agency collaborations and initiatives.

1.5.2 Agency Privacy Policies, Protocols and Practices

This Policy sets forth the baseline requirements for City agencies relating to the protection of identifying information. City agencies may adopt supplemental privacy policies and protocols that address topics specific to the unique needs of their agency and the agency's clients, or to comply with applicable laws and regulations governing the identifying information collected, used, disclosed, or retained by the agency and its contractors and subcontractors. In the event of conflict, agency privacy policies and protocols that are more stringent than this Policy shall take precedence.

Agency privacy officers must issue guidance to their agency's employees, and to covered contractors and subcontractors, regarding the agency's collection, retention, and disclosure of identifying information. Refer to **Section 4.2** of this Policy for more information on agency privacy officer responsibilities.

1.5.3 Citywide Information Technology and Security Policies and Standards

The City's Information Technology Security Policies and Citywide Technology Policies and Guidelines, as they now exist and may be from time to time amended, are issued by the New York City Cyber Command ("Cyber Command") and the Department of Information Technology and Telecommunications ("DoITT") (collectively, the "Citywide IT Policies").[7] These policies relate to the classification, transfer, and storage of identifying information. The following Citywide IT Policies are especially relevant to the proper handling and protection of identifying information:

- Data Classification Standard
- Encryption Policy
- Encryption Standard
- Digital Media Re-use and Disposal Policy
- User Responsibilities Policy Citywide Incident Response Planning (P-IR-01)
- Agency Incident Response Plan
- Portable Data Security Policy
- Citywide Cloud Policy[8]

[6] One New York: The Plan for a Strong and Just City ("OneNYC") is the City's comprehensive 10-year plan establishing bold goals and specific targets for a sustainable, resilient City for all New Yorkers, which includes an express initiative to expand the City's internal data integration capacity.

[7] All Citywide IT Policies are available on Cityshare. Agencies must also comply with any agency specific security policies.

[8] The Citywide Cloud Policy requires that City agencies and entities submit any plans to use cloud services to DoITT for review to ensure that appropriate security, legal, and operational measures are considered.

Identifying information that is determined to be "sensitive identifying information"[9] should receive the appropriate level of security protection, whether in physical or electronic format. It should not be stored or transmitted across any communication mechanism unless it is protected using approved data encryption technology or other secure means. This includes storing identifying information in secure databases or on secure file servers using the appropriate encryption protocol reflected in the Citywide Encryption Standard.

Agency privacy officers should coordinate with relevant agency IT/MIS units, Cyber Command and DoITT, as needed, to: (1) identify and address the impact of any technical requirements for the agency's collection, retention, and disclosure of identifying information in accordance with the Citywide IT Policies; (2) identify agency specific information technology and security policies;[10] and (3) ensure that any guidance issued by agency privacy officers to their agency's employees in furtherance of compliance with the Identifying Information Law or this Policy incorporates information on relevant sections of the Citywide IT Policies, agency specific information technology and security policies, and any additional guidance from relevant IT/MIS leadership, Cyber Command, and DoITT, and provides appropriate guidance to their covered contractors and subcontractors.

1.5.4 Mayoral Directive 2015-3: Uniform Records Management Practices

City agencies must retain identifying information where required by law and may retain identifying information to further the mission or purpose of the agency, or where retention is in the interests of the City, is not contrary to the purpose or mission of the agency, and is otherwise permitted by law.[11] Agency compliance with Mayoral Directive 2015-3,[12] which sets forth the City's Uniform Records Management Practices, is determined as being in the interests of the City. Agencies are responsible for compliance with applicable information retention requirements, including but not limited to the agency's Records Retention and Disposition Schedule approved by the Department of Records and Information Services ("DORIS") in accordance with Mayoral Directive 2015-3. See **Section 5.7** for requirements on Retention of Identifying Information.

1.5.5 Model Protocols for Handling Third Party Requests for Information Held by City Agencies

City agencies should follow the Model Protocols for Handling Third Party Requests for information Held by City Agencies ("Model Protocols"), issued as City policy in April 2017 by the First Deputy Mayor.[13] The Model Protocols set forth a factual and legal assessment process which agencies must follow when handling a request from a third party for City information, including but not limited to identifying information. Agencies must either adopt the Model Protocols in their entirety, or develop and adopt a comparable protocol.[14]

1.5.6 General Confidentiality Policy

Executive Order Numbers 34 and 41 of 2003 (together, the "General Confidentiality Policy") comprise a City privacy policy that restricts the collection and disclosure of certain identifying information designated as "confidential." Specifically, Executive Order 41 of 2003 establishes restrictions on City officers' and employees' disclosure of "any information obtained and maintained by a City agency relating to an individual's sexual orientation, status as a victim of domestic violence, status as a victim of sexual assault, status as a crime witness, receipt of public assistance, or

[9] See **Section 3.2.6** of this Policy.
[10] Relevant agency-specific policies may include Acceptable Use policies, Acceptable Email Usage Policies, IT and Equipment Policies, and Remote Access Policies which may address an employee's use of City- or agency-issued devices, as well as an employee's use of personal devices or e-mail addresses for City business.
[11] See Admin. Code § 23-1202(e).
[12] See Section 6 of Mayoral Directive, available at https://www1.nyc.gov/site/records/about/records-management-policies.page.
[13] The Model Protocols are on file with the Mayor's Office of Information Privacy.
[14] Email directive on file with the Mayor's Office of Information Privacy.

immigration status [and] all information contained in any individual's income tax records." Executive Order 41 also amends Executive Order 34 of 2003, and directs City officers and employees not to inquire about individual's immigration status unless an exception set forth in the orders applies. The General Confidentiality Policy is consistent with the requirements of the Identifying Information Law and this Policy in that, taken together, they create a comprehensive, citywide framework for privacy protection and best practices by City agencies in relation to the collection and disclosure of the personal information of New Yorkers.

1.6 Relationship of the Identifying Information Law to Other Laws

Where a federal or state law or regulation conflicts with the Identifying Information Law on the same subject matter, the federal or state law or regulation will govern. Questions about the applicability of other laws (including local laws and regulations) should be directed to the agency's privacy officer or general counsel, the Chief Privacy Officer, or the City's Law Department.

1.6.1 New York State Freedom of Information Law

The New York State Freedom of Information Law ("FOIL") establishes a process for members of the public to request copies of records, and establishes a duty for City agencies to disclose such records in response to a request unless an exception applies.[15] Such records may include identifying information. When FOIL, a state law, requires an agency to disclose identifying information, the agency should disclose it and will not need to comply with the Identifying Information Law with respect to that disclosure. When an exception to the disclosure requirements under FOIL is applicable, but the agency is considering whether to voluntarily disclose the requested identifying information, the agency will need to comply with the Identifying Information Law.[16] Refer to **Section 4.1.1.1** relating to the Records Access Officer.

1.6.2 Open Data Law

Local Law 11 of 2012 (the "Open Data Law"), as amended,[17] mandates that all public data sets be made accessible on a single web portal by the end of 2018. Determinations as to when identifying information constitutes a "public data set"[18] involves a legal determination that should be made in consultation with the agency privacy officer or other designated agency counsel before such information is made publicly available.

1.6.3 Local Law 45 of 2005 and Local Law 11 of 2017

Local Law 45 of 2005 and Local Law 11 of 2017, codified at Admin. Code §§ 10-501 et seq., set forth requirements for City agencies to follow in the event that an agency disclosure of "personal identifying information"[19] constitutes a "breach of security."[20] Where identifying information meets the definition of personal identifying information and the disclosure constitutes a breach of security, agencies are required to follow the procedures set forth in Admin. Code § 10-502. Refer to **Section 8.3** on relevant notification requirements.

[15] See Article 6 of the N.Y.S. Public Officers Law.
[16] For additional guidance on the relationship of the Identifying Information Law to other laws and regulations, contact appropriate agency counsel, the Chief Privacy Officer or the Law Department, as needed.
[17] See Admin. Code §§ 23-501 et seq.
[18] See Admin. Code § 23-501(g) for a definition of "public data set."
[19] See Admin. Code § 10-501(a).
[20] See Admin. Code § 10-501(b).

2.0 Privacy Principles

The City of New York has an ongoing responsibility to safeguard the identifying information of its employees, officials, and members of the public that is maintained by City agencies, while also fulfilling its mandate to provide important City services and resources, which often requires the coordination and sharing of personal information across agencies and with other parties. With advances in technology, the increasing volume of electronic transactions involving such information calls for robust privacy protection and data security practices to guard against the unauthorized access, fraud, theft, and other misuse of such information.

In meeting such obligations and new challenges, City agencies should adhere to the following privacy protection principles ("Privacy Principles"), as they strive to balance privacy protections with the importance of responsible data sharing, where permitted by law, to provide benefits, services, and care to individuals and families who need them, advance and improve coordination of multiagency initiatives that deliver health and human services and strengthen City infrastructure, help ensure public safety, and improve economic outcomes.

City agencies should incorporate these Privacy Principles into all aspects of agency decision-making and operations where individuals' privacy interests are implicated, whether directly or indirectly, including but not limited to: when developing partnerships with private entities; providing programs and services; conducting agency rulemaking; developing technical systems and solutions; and engaging in other types of agency policy and decision-making that may have privacy implications.

	Privacy Principle	**Description**
1	Accountability	City agencies should establish and implement agency privacy protection policies and protocols, develop strategies and plans to periodically assess and modify such practices as privacy and security threats emerge and evolve, and guide its covered contractors and subcontractors in such efforts.
2	Public Trust	City agencies and their covered contractors and subcontractors should collect, use, retain, and disclose identifying information in a manner that protects an individual's privacy interests to the greatest extent reasonable under the circumstances so that all members of the public can seek and safely access needed City services and resources, trusting that the City is appropriately safeguarding their personal information.
3	Responsible Governance and Stewardship	In delivering necessary City services and striving to improve outcomes for its residents, City agencies and their covered contractors and subcontractors should appropriately protect the privacy and security of identifying information so that such information is used collected, accessed, stored, and disclosed or otherwise shared only with authorized persons for lawful purposes.
4	Data Quality, Integrity, and Accuracy	City agencies should endeavor to maintain identifying information in a manner that protects its quality, integrity, and accuracy. Agencies should take reasonable steps to ensure that inaccurate or outdated identifying information is corrected, updated, or, where appropriate, securely disposed.
5	Security Safeguards	City agencies and their covered contractors and subcontractors should use appropriate safeguards in both physical and virtual places to protect identifying information from unauthorized access and disclosure, in accordance with applicable laws, regulations, and City and agency policy.

Mayor's Office of Information Privacy

3.0 Definitions and Key Terms

3.1 Definition of Identifying Information

"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.[21] The Identifying Information Law enumerates the types of information listed in the below chart. These enumerated types of identifying information represent a non-exhaustive list of information that constitutes identifying information. Agencies should construe the definition of identifying information so that any information that alone or in combination with other information can identify or locate an individual is afforded appropriate privacy protection.

Enumerated Types of Identifying Information:

- Name
- Place of birth
- Current and previous home and work addresses
- Gender identity
- Race
- Marital or partnership status
- Sexual orientation
- Contact information such as phone number or email address
- Citizenship or immigration status
- Nationality
- Country of origin
- Languages spoken
- Religion
- Employment status
- Employment information
- Motor vehicle information or license plate number
- Biometrics such as fingerprints or photographs
- Information concerning social media accounts
- All information obtained from an individual's income tax records
- Eligibility for and receipt of public assistance or city services
- Status as a victim of domestic violence or sexual assault
- Status as a crime victim or witness
- Arrest record or criminal conviction
- Date and/or time of release from custody of ACS, DOC or NYPD
- Any scheduled court appearances
- Information obtained from any surveillance system operated by, for the benefit of, or at the direction of NYPD
- Any scheduled appointments with any employee, contractor or subcontractor

3.1.1 Additional Types of Identifying Information Designated by the Chief Privacy Officer

Pursuant to Charter § 8(h)(4), the Chief Privacy Officer may designate additional types of information that must be subject to protection by City agencies, and certain City agency contractors and subcontractors, based on the nature of such information and the circumstances of its collection or potential disclosure. Accordingly, the Chief Privacy Officer has designated the following additional types of information for protection:

- Date of birth
- Social security number (including last 4 numbers)
- Internet protocol address
- Device identifiers including media access control (MAC) address or Internet mobile equipment identity (IMEI)
- GPS-based location obtained or derived from a device that can be used to track or locate an individual

Agencies are advised to update applicable routine designations, as necessary, to reflect these additional types of identifying information designated by the Chief Privacy Officer, if the agency collects, retains, or discloses such information.

[21] Admin. Code § 23-1201.

3.1.2 Guidance in Determining when Other Information Constitutes Identifying Information

Unless information has been clearly designated as a type of "identifying information" under Admin. Code § 23-1201 or by the Chief Privacy Officer, determining whether or not information meets this definition can depend on the facts and circumstances in which the information is being collected or disclosed. In making a determination as to whether particular information can by itself or combination with other information identify or locate a person, it may be useful to consider the type and volume of data elements at issue along a continuum: the more data elements/types that can be strung together, the more likely it may be that a person can be identified or located. As an example, in determining whether "zip code" constitutes identifying information for a data analytics project evaluating an agency program, consider whether it is possible that less than five individuals meeting the program's criteria reside within a particular zip code, where other information is also available about the individual, such as program affiliation and other physical descriptors. In this instance, zip code may be considered identifying information because it can be used, in combination with the other available information, to identify or locate a particular person.

3.2 Clarification of Terms Not Defined in the Identifying Information Law

3.2.1 Anonymization

In relation to the Identifying Information Law and this Policy, "anonymization" shall be understood to mean the measures taken to minimize and, where feasible, remove the elements of information that identify an individual, whether contained in data sets, records, or other mediums, including but not limited to de-identification, pseudonymisation, redaction, encryption, masking, and hashing.

3.2.2 Collection

"Collection" shall be understood to mean the act of directly or indirectly receiving, retrieving, extracting, and/or accessing information from a person, government entity, agency or office, private entity, contractor or subcontractor, or system. An affirmative act by the agency is required. Where an agency serves solely as a technical conduit for the identifying information (e.g., an agency providing the technical infrastructure for transmitting information), this is not considered a "collection." Such an exception should be understood to apply only to very limited number of agencies, such as DoITT.

3.2.3 Disclosure

"Disclosure" shall be understood to mean the act of releasing, transferring, disseminating, providing access to, or divulging identifying information in any manner, whether inadvertently or intentionally, outside of the agency. Where an agency serves solely as a technical conduit for the identifying information (e.g., an agency providing the technical infrastructure for transmitting information), this is not considered a "disclosure." Such an exception should be understood to apply only to very limited number of agencies, such as DoITT.

3.2.4 Exigent Circumstances

While not defined in the Identifying Information Law, "exigent circumstances" shall be understood to mean circumstances when a collection or disclosure of identifying information is urgently necessary, such that procedures that would otherwise be required, such as prior review and approval by the agency privacy officer or Chief Privacy Officer, might cause undue delays. Refer to **Section 5.4** for requirements for collections and disclosures under exigent circumstances.

3.2.5 Sensitive Identifying Information

"Sensitive" identifying Information refers to certain types of identifying information which the agency privacy officer or Chief Privacy Officer has determined that alone, or in combination with other information may, based upon their very nature or under specific facts and circumstances, pose a higher risk of harm to an individual or members of an individual's household, such as but not limited to identity theft, danger to health and safety, severe financial loss, reputational harm, or other harms dependent upon any protected status of an individual, if such information were to be improperly disclosed, whether inadvertently or intentionally, to unauthorized persons. Refer to **Section 3.1** for the definition of "identifying information" and **Section 5.5.1** for requirements for requests and proposals involving sensitive identifying information.

3.2.6 "Requests" and "Proposals" for Identifying Information

The Identifying Information Law refers to "requests" and "proposals" for identifying information in Admin. Code §§ 23-1205(a)(1)(c)(1) and (2). While not defined the law, these terms shall be understood to have the following meanings:

- **"Requests"** for identifying information shall mean requests for the release or production of identifying information by a third party, such as but not limited to: press/media inquiries; FOIL requests; judicial and administrative subpoenas; City agency requests for identifying information from another agency; requests from a law enforcement official or agency in relation to an investigation; requests from an elected official for oversight purposes; and information that is available to the public pursuant to Admin. Code §23-501 et seq.

- **"Proposals"** for identifying information shall mean requests for identifying information for a new project that involves data integration, analysis, or research, and other similar projects and other new initiatives that involve a the proposed sharing of an agency's identifying information across agencies, or with other entities outside of the agency for a particular proposed purpose or project.

Refer to **Section 5.5** for requirements regarding requests and proposals for identifying information.

4.0 Agency Privacy Officer

4.1 Designation

The Identifying Information Law requires each agency head to designate an individual to act as its privacy officer. When an agency designates a new privacy officer, the agency must promptly notify the Chief Privacy Officer at PrivacyOfficer@cityhall.nyc.gov and provide relevant business contact information for the new agency privacy officer.

4.1.1 Agency Employee Designations

While not mandated by the Identifying Information Law, it is strongly recommended that the agency privacy officer designated be an attorney. Agency privacy officers who are not attorneys should consult with their agency's general counsel or the City's Law Department before making any determinations regarding identifying information that may have legal implications.

4.1.1.1 Records Access Officer

Where a disclosure of identifying information is made in response to a request pursuant to the FOIL, the agency's records access officer may perform the functions otherwise performed by the agency privacy officer with respect to such request.[22]

[22] See Admin. Code § 23-1201. Refer to **Section 1.6.1** on the relationship of FOIL to the Identifying Information Law.

4.1.2 Contractors and Subcontractors

When a covered contractor or subcontractor is required to comply with the Identifying Information Law, the agency may designate such contractor or subcontractor to perform the duties of the agency privacy officer with respect to the specific contract or subcontract.[23] If the agency makes such a designation, the covered contractor or subcontractor will be responsible for the certain privacy officer functions described in **Section 4.2** below for the designated contract or subcontract. Contractors or subcontractors that are authorized by the agency to perform the duties of the agency privacy officer must also comply with requirements this Policy, as it may be from time to time amended.

4.2 Agency Privacy Officer Responsibilities

4.2.1 Agency Privacy Protection Policies and Guidance

The Identifying Information Law requires agency privacy officers to compile and report certain information about the agency's policies and practices regarding its collection, retention, and disclosure of identifying information. Agency privacy officers must adopt this Policy as a baseline for the protection of identifying information maintained by their agency, and for the compilation and reporting[24] of certain information regarding such policies.

Agency privacy officers or other designated agency counsel must issue and arrange for dissemination of guidance to the agency's employees and covered contractors and subcontractors on the mandates of this Policy, as it may from time to time be amended, and the Identifying Law's requirements relating to the collection, retention, and disclosure of identifying information.[25] Agency privacy officers or other designated agency counsel may also, in consultation with the agency head and agency's legal office, issue additional agency specific guidance, policies, and protocols that are no less restrictive than this Policy with respect to privacy and security protection requirements, and compliant with applicable laws and regulations affecting the agency. The Mayor's Office of Information Privacy will issue model guidance that agencies can adopt or adapt to fulfill the requirements of this section.

4.2.2 Agency Compliance Plan

Agency privacy officers should develop a plan for compliance with the Identifying Information Law and this Policy.[26] The Mayor's Office of Information Privacy will issue guidance that agencies can adapt in developing and implementing such plans.

4.3 Approval of Collections and Disclosures

4.3.1 Pre-approval as Routine

Agency Privacy Officers are authorized under the Identifying Information Law to pre-approve certain collections and disclosures of identifying information as "routine."[27] Such designations are necessary to ensure that the agency's collections and disclosures of identifying information in conducting their normal business operations may continue in accordance with the requirements of this law, and without interruption. Refer to **Section 5.1** on routine designations.

[23] See Admin. Code § 23-1202(g).
[24] See Admin. Code § 23-1205.
[25] See Admin. Code § 23-1203(2).
[26] See Admin. Code § 23-1203(8).
[27] See Admin. Code §§ 23-1202(b)(2)(a), 23-1202(c)(2)(a).

4.3.2 Approval on a Case-by-Case Basis of Collections and Disclosures that are not "Routine"

Agency privacy officers may, on a case-by-case basis, approve a collection or disclosure of identifying information if the collection or disclosure furthers the purpose or mission of the agency, or is required by law or treaty.[28] Such approvals must be documented by the agency privacy officer and communicated to the relevant agency staff and covered contractors and subcontractors. Examples of case-by-case approvals may include but are not limited to unique data integration analytic or research projects, or a disclosure of identifying information in response to a specific request, such as a press inquiry.

4.3.3 Exemption for Collections and Disclosures Involving Investigations

There is a categorical exemption to the Identifying Information Law's general requirement that, absent exigent circumstances, either the agency privacy officer or chief privacy officer must approve collections and disclosures of identifying information. Specifically, neither agency privacy officer nor Chief Privacy Officer approval is required where: (i) identifying information is collected or disclosed by the New York City Police Department in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime, or (ii) the collection or disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individually who is otherwise not legally competent.[29]

4.4 Reporting

4.4.1 Agency Reports

The Identifying Information Law requires agencies to submit a biennial report by July 31st beginning in 2018, containing certain detailed information about their agency's collection and disclosure of identifying information and their privacy practices.[30] The agency privacy officer should work with the agency head or their designee to support agency compliance with this obligation.[31] The agency may opt to submit additional information as the agency head believes is necessary for the report.

4.4.2 Quarterly Report on Unauthorized Disclosures and Collections and Disclosures Made Under Exigent Circumstances

Agency privacy officers are responsible for gathering information from relevant personnel on any disclosures made in violation of the Identifying Information Law or any collections or disclosures made under exigent circumstances. All such information gathered from agency personnel must be reported on a quarterly basis to the Chief Privacy Officer, starting with the first quarter ending September 15, 2018. To assist agency privacy officers in fulfilling this obligation, the Chief Privacy Officer, through the Mayor's Office of Information Privacy, has issued guidance which may from time to time be amended. Based upon such information reported by agencies, the Chief Privacy Officer creates and submits an anonymized compilation or summary of such disclosures made in violation of the Identifying Information Law and under exigent circumstances to the Speaker of the Council, and makes such report available online.[32]

Agency privacy officers must notify the Chief Privacy Officer as soon as practicable when an individual's identifying information is either disclosed in violation of the Identifying Information Law, or collected or disclosed under exigent

[28] See Admin. Code § 23-1202.
[29] See Admin. Code §§ 23-1202 (b)(2)(c) and (c)(2)(c).
[30] See Admin. Code § 23-1205.
[31] Guidance in meeting this requirement is on file with the Mayor's Office of Information Privacy.
[32] See Admin. Code §§ 23-1202(c)(4), 23-1202(d)(2). CPO reports are currently posted online via the Mayor's Office of Information Privacy website.

circumstances.[33] Agency privacy officers should also notify the agency's general counsel or other agency counsel of any suspected or known violation. Refer to **Section 8.0** for further information on receiving and investigating complaints for violations of the Identifying Information Law.

5.0 Agency Collection, Retention and Disclosure of Identifying Information

5.1 Routine Collections and Disclosures of Identifying Information

Generally, agency privacy officers are responsible for reviewing all collections and disclosures of identifying information made by the agency and designating relevant collections and disclosures as "routine" so that the agency may continue its normal business operations involving identifying information. In order for collections or disclosures to be designated and pre-approved by the agency privacy officer as "routine," they must meet a two-part test, in that they must: (1) be "made during the normal course of city agency business"; and (2) "further the purpose or mission" of the agency.[34] Agency privacy officers must document the collections and disclosures they have designated as routine and agencies must advise the appropriate agency staff, covered contractors and subcontractors of such pre-approvals.[35]

5.1.1 Pre-approval as Routine by Agency Privacy Officers of Two or More Agencies

A "routine" collection or disclosure may include collections and disclosures that occur between two or more City agencies when the respective agency privacy officers agree that the collection or disclosure furthers the purpose or mission of their respective agencies.[36] Examples may include ongoing transmissions of data between agencies for a specific purpose involving two agencies (such as where Agency A and Agency B regularly exchange identifying information with each other to administer a benefit program or service), or to manage a mutually dependent, ongoing interagency function such as payroll operations, or to comply with the agency's records retention policy.

Where a collection or disclosure of identifying information has been pre-approved as "routine" by two or more agency privacy officers, the privacy officers may coordinate with each other to document the arrangement in required agency reporting. With respect to such reports, each agency (or agencies) disclosing the information and each agency (or agencies) collecting the information should have complementary descriptions in such reports that are consistent with respect to the arrangement (i.e., where Agency A is disclosing the information to Agency B, then Agency A should designate/report the disclosure as "routine" and Agency B should designate/report the collection of the same information from Agency A as "routine). These agency privacy officers' pre-approvals must be communicated to the relevant agency staff and covered contractors and subcontractors at each respective agency.

Agency privacy officers are not required to use this complementary approach for making routine designations involving two or more agencies, especially where it may be burdensome to coordinate such documentation and reporting among a significant number of agencies. Agency privacy officers may instead rely on their authority to approve collections and disclosures as "routine" as otherwise described in this section.

5.1.2 Guidance for Making "Routine" Designations by Agency Function

Agency privacy officers may designate as "routine" collections and disclosures made in connection with an agency function. Examples of such functions include but are not limited to Legal Services, Personnel Administration, Communications, or Constituent Affairs. Even where an Agency Privacy Officer has pre-approved certain collections and

[33] See Admin Code § 23-1202(d)(1).
[34] See Admin. Code § 23-1201.
[35] Guidance in meeting this requirement is on file with the Mayor's Office of Information Privacy.
[36] See Admin. Code § 23-1201.

disclosures for agency functions as routine, agency personnel should strive to collect or disclose identifying information which is needed to reasonably accomplish the agency function, in accordance with **Section 5.5** below.

In cases where the agency privacy officer has designated as "routine" certain functions involving collections and disclosures that meet the above referenced two-part test, where the function requires the agency to disclose identifying information to a third party, the agency privacy officer or other designated agency counsel should ensure that a protocol is implemented so that any identifying information collected or disclosed in relation to such requests is in accordance with the requirements of applicable law and regulations, and this Policy. The agency may adopt the Model Protocols to meet this requirement. Such protocol should be incorporated into agency guidance referenced in **Section 4.2.1** of this Policy.

5.1.3 Support in Making Agency Routine Designations

While authority to designate a collection or disclosure as routine rests with the agency privacy officer, the Chief Privacy Officer or City's Law Department may be consulted where the agency privacy officer is unsure whether a certain collection or disclosure should be designated as routine for their agency. In such instances, the agency privacy officer may also consult with the Chief Privacy Officer as to whether the Chief Privacy Officer can approve such collection or disclosure as being in the best interests of the City.

5.2 Agency Privacy Officer Approval of Collections and Disclosures of Identifying Information on a Case-by-Case Basis

An agency privacy officer may also approve collections and disclosures of identifying information on a case-by-case basis where the collection or disclosure has not been designated as "routine" but such collection or disclosure is either required by law or furthers the purpose or mission of the agency.[37] Such collections and disclosures are considered "non-routine." An example is where the agency privacy officer approves a disclosure of identifying information for a unique data-sharing initiative or multi-agency study involving one or more other agencies.[38]
When a request is received for collection of disclosure of identifying information that has not been designated as "routine," the collection or disclosure is not required by law, and the agency privacy officer has not determined that it furthers the purpose or mission of the agency, the request should be denied or referred to the Chief Privacy Officer, who may approve collections of identifying information upon a determination that the collection is in the best interests of the City, and approve disclosures of identifying information between City agencies as being in the best interests of the City.[39] Refer to **Section 5.2.3** on the Chief Privacy Officer's role in non-routine collections and disclosures. Note, that there is overlap between the types of disclosures and collections that can be approved by the Chief Privacy Officer and those that can be approved by the agency privacy officers. Agency privacy officers may contact the Chief Privacy Officer if they have any questions or concerns about case-by-case requests for identifying information.

5.2.1 Considerations in Determining Whether a Collection or Disclosure is "Routine" or "Non-Routine"

In considering whether a certain collection or disclosure should be pre-approved as "routine" or treated as "non-routine," agency privacy officers may consider the below criteria, as well as other factors based on their agency's mission and purpose. If the majority of considerations listed below weigh toward the negative (i.e., answer of "no"), the agency privacy officer should consider the collection or disclosure as "non-routine" and review it on a case-by-case basis.

- Is the collection or disclosure one that is or will be frequently performed by the agency?
- Does the collection or disclosure involve or require a recurring action or function of the agency?

[37] See Admin. Code § 23-1202(c)(3).
[38] Further guidance on such designations is on file with the Mayor's Office of Information Privacy.[39] See Admin. Code §§ 23-1202(b)(2)(b), 23-1202(c)(2)(b).
[39] See Admin. Code §§ 23-1202(b)(2)(b), 23-1202(c)(2)(b).

- Is the collection or disclosure consistent with the stated purpose or mission of the agency in its communications, guidance and policy documents, on its website and in other agency materials, or in applicable laws and regulations?
- Is the collection or disclosure made in the ordinary course of the agency's daily business?
- Is the type of requesting entity involved with the normal business operations of the agency?
- Is the purpose of the request, and any anticipated or possible future use of the information, required by law or regulation, or otherwise related to the agency's purpose or mission?
- Are there unique facts or circumstances regarding the collection or disclosure, given the proposed purpose and anticipated user of the information that would not be consistent with the purpose or mission of the agency?

5.2.2 Guidance for Responding to Requests for Identifying Information from Oversight Agencies

Since oversight agencies regularly request information (that may include identifying information) pursuant to their authority under the Charter, Administrative Code, or other applicable provision of law, agency privacy officers may be able to designate disclosures made in response to such lawful requests as "routine" provided that the requestor's authority in relation to the information requested is not superseded by a federal or state law restricting the disclosure. Agency privacy officers may also be able to approve such disclosures as required by law or treaty.

5.2.3 Chief Privacy Officer Role in Non-Routine Collections and Disclosures

The Chief Privacy Officer may approve in advance: (i) collections of identifying information upon the determination that such collection is in the best interest of the City, and (ii) disclosures to another City agency or City agencies upon determination that such disclosure is in the best interest of the City. An example of this "best interests" determination by the Chief Privacy Officer might be a citywide or multi-agency data-sharing project that the agency privacy officer does not believe furthers the purpose or mission of the privacy officer's agency, but the disclosure of identifying information between and among multiple agencies for this initiative serves a broader City purpose of enhancing the health, welfare, or safety of New Yorkers, provided that the disclosure of such information is not otherwise restricted by law. The agency privacy officer should consult with the Chief Privacy Officer as appropriate to refer such matters for best interests of the City determination.

5.3 Collections and Disclosures Involving Investigations

The approval of an agency privacy officer is not required for collections and disclosures by or to the New York City Police Department in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime, or where the collection or disclosures is in connection with an open investigation by a City agency concerning the welfare of a minor or an individually who is otherwise not legally competent.[40]

5.4 Collections and Disclosures made under Exigent Circumstances

Agencies and their covered contractors and subcontractors are authorized under the Identifying Information Law to make collections and disclosures of identifying information under exigent circumstances. While "exigent circumstances" is not defined in the Law, it should be understood to mean those emergency type circumstances where it is not practicable to consult in advance with the agency privacy officer regarding such collection or disclosure, restricted in duration as necessary to resolve the urgency, and not a blanket exception to the otherwise required procedures of agency privacy officer or Chief Privacy Officer review and approval.

Information about the collection or request and disclosure made under exigent circumstances, along with an explanation of why exigent circumstances exist, must be reported to the agency privacy officer as soon as practicable after such

[40] See Admin. Code §§ 23-1202 (b)(2)(c) and (c)(2)(c).

collection or disclosure to the agency privacy officer, who in turn must report such information to the Chief Privacy Officer as soon as practicable, except where such notification is expressly exempted under Admin. Code §§ 23-1202(d)(1)(a)–(c).

5.5 Requests and Proposals for Identifying Information

In responding to requests and proposals for disclosure of identifying information to third parties, agencies should refer to the Model Protocols.[41] Proposals for identifying information may require on-going transmission or disclosure requiring additional agency resources. For example, a proposal may involve weekly transmission of updated data files, or require electronic data matching capability for which the agency lacks technical resources to do so. When reviewing such proposals, agency privacy officers should collaborate as needed with relevant agency counsel and programmatic and technical leads to determine legality and operational and technical feasibility of the proposal.

5.5.1 Requests and Proposals for Sensitive Identifying Information

Requests or proposals for the collection or disclosure of sensitive identifying information shall require additional review by the agency privacy officer, or designated agency counsel, and the Chief Privacy Officer, unless such collection or disclosure has been designated as "routine" by the agency privacy officer, or by the Chief Privacy Officer as in the best interests of the City.

5.6 Data Minimization

City agencies and their covered contractors and subcontractors should strive to minimize the collection and disclosure of identifying information where possible to achieve the purposes reasonably necessary to accomplish the legal or operational purpose of such collection or disclosure, keeping in mind the importance of balancing privacy protection with the important work of agencies and their contractors and subcontractors that requires cross-agency collaboration and coordination. Agency policies should encourage agency employees to consult with the agency privacy officer to determine ways in which disclosure of identifying information can be responsibly minimized where appropriate and reasonably feasible, and should advise their covered contractors and subcontractors on such strategies.

5.6.1 Anonymization

Anonymization is a practice by which agencies minimize the identifying elements of information whether contained in data sets, records, or other mediums. Agency privacy officers should consult with agency leadership to assist in identifying circumstances where it is appropriate, given the purpose and mission of the agency, to anonymize information. Where such circumstances have been identified, agency privacy officers should work with technical staff to implement appropriate methods of anonymization, which may include but are not limited to de-identification, pseudonymisation, redaction, encryption, masking, and hashing. Other strategies, such as limiting disclosure of identifying information by using values of <5 or <10 may also be useful in certain circumstances, such as reporting or evaluation. Note that "anonymization" and "de-identification" may have specific definitions in other contexts, including under other laws and regulations; agency privacy officers should consult with the Chief Privacy Officer or the Law Department as necessary to determine the applicability of any such requirements under such laws or regulations.

[41] Refer to **Section 1.5.5** for information on the Model Protocols.

5.7 Retention of Identifying Information

Pursuant to Admin. Code § 23-1202(e), agencies must retain identifying information where required by law or City and/or agency policy. Any identifying information contained in agency records subject to the agency's Records Retention and Disposition Schedule must be retained in accordance with the applicable period of time set forth therein, in addition to other laws, regulations, or policies applicable to the City agency. No agency records that are subject to the records retention and disposition schedule may be destroyed or otherwise disposed of by an agency unless prior approval has been obtained from the Commissioner of DORIS, the Corporation Counsel for the City of New York, and the agency head that created or has jurisdiction over the records.

Additionally, agencies may retain identifying information to further its mission or purpose, or where retention is in the best interest of the City, is not contrary to the agency's mission or purpose, and is permitted by law. Agency privacy officers, in consultation with their agency's general counsel or other agency counsel and records management officer, can determine whether the retention of identifying information furthers their agency's mission or purpose. Agency privacy officers or other designated agency counsel should coordinate with their agency's records officer to ensure that appropriate agency staff are advised of permissible retention policies and practices related to the Identifying Information Law. Even where certain agency records that contain identifying information are required to be retained in accordance with applicable laws, regulations, or policies, agencies should consider limiting access to such records to staff responsible for their storage and maintenance.

5.7.1 Data Storage and Maintenance Requirements

Identifying information retained by the agency should be stored and maintained in accordance with the Citywide Data Classification Standards, applicable Citywide IT Policies, and this Policy.

5.7.2 Disposal of Identifying Information

Identifying Information and records containing identifying information should be disposed of in a manner that prevents, or otherwise minimizes the risk of unauthorized or inadvertent disclosure of such information, in accordance with any applicable laws, regulations, or policies.[42] The agency privacy officer should coordinate with the agency records access officer with respect to disposal of identifying information.

Where agency staff, or covered contractors, or subcontractors discover that disposal of identifying information has or may have occurred in a way that could have disclosed identifying information in violation of the Identifying Information Law, this Policy, or any other applicable laws, regulations or policies, such agency staff must promptly notify their agency privacy officer in accordance with agency policy and protocol.

6.0 Contracts

6.1 Contractors and Subcontractors Subject to the Identifying Information Law

Covered contractors and subcontractors must comply with the Identifying Information Law. Covered contracts must include the "Identifying Information Rider," which is attached to this Policy and on file with the Mayor's Office of Information Privacy and the Law Department (see **Appendix B**). This Rider supplements the City Standard Human Services Contract, the Discretionary Fund Contract for human services less than $100,000, other human services contracts, and other contracts for services designated by the Chief Privacy Officer.

[42] When disposing of records containing identifying information or certain electronic equipment, agencies should be aware of potential obligations under Admin. Code §§ 10-503, 10-504, in addition to any other applicable laws, regulations, or policies.

6.1.1 Contractors and Subcontractors Subject to the Identifying Information Law

The Identifying Information Law expressly applies to contractors and subcontractors for human services.[43] Human services means 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.[44]

6.1.2 Contracts and Subcontracts for Other Services Designated by the Chief Privacy Officer

The Chief Privacy Officer, through the Mayor's Office of Information Privacy, will collaborate with the Law Department, Mayor's Office of Contract Services, and other relevant agencies to identify contracts and subcontracts for other services that require additional contractual privacy protections, and determine the most appropriate way to incorporate such protections. Types of additional contracts for services under review by the Chief Privacy Officer include those where contractors or subcontractors have direct access to the sensitive identifying information of New Yorkers, and contracts for which "Appendix A: General Provisions Governing Contracts for Consultants, Professional, Technical, Human, and Client Services" is not required. Guidance on requirements for such contracts and subcontracts for other services will be communicated by the Chief Privacy Officer to agency heads and agency privacy officers.

6.2 Requirements for Data Sharing Agreements

6.2.1 When an Agreement is Required

Absent exigent circumstances, when an agency makes a disclosure of identifying information to another agency that its agency privacy officer has not designated as "routine," the agency should enter into a data sharing agreement with the agency collecting the information unless the agency privacy officer, in consultation with the Chief Privacy Officer as necessary, determines that such an agreement is not required because there is not a risk that an important privacy interest will be compromised.

Even where certain disclosures of identifying information have been designated as "routine," because of the nature or extent of such disclosures, or because of the nature of the relationship of the City agency and the third party, the disclosing City agency must enter into a data sharing agreement with such third party in certain circumstances.[45] Agency staff should consult with their agency privacy officer or the Chief Privacy Officer to identify when a disclosure involving a third-party will require an agreement. Such circumstances may include, but are not limited to:

- Disclosures of "sensitive" identifying information, where determined by the Chief Privacy Officer or the agency privacy officer;
- Disclosures of identifying information that are restricted by other laws or regulations;
- Disclosures transferring custody and maintenance of identifying information to a third party;
- Disclosures to a third-party requiring additional contractual protections, such as but not limited to insurance, intellectual property and ownership, and indemnification.

When a law, regulation, or oversight agency requires a particular form for a data sharing agreement, City agencies should follow such requirements when complying with this section. When no such requirements are applicable, agencies should refer to the Citywide Data Integration Initiative, which establishes a legal framework that includes privacy and security

[43] See Admin. Code § 23-1201.
[44] See Admin. Code § 23-1201; 6-129(c)(21).
[45] See Admin. Code § 23-1203(4).

protection protocols for data sharing, and leverages secure technical resources to advance the City's capacity for data integration, research and analytic work, in accordance with applicable laws and regulations.[46]

6.2.2 Elements of Data Sharing Agreements

Each data sharing agreement involving identifying information should take into consideration the unique facts and circumstances involving the data sharing, including but not limited to the types of identifying information and other data being shared, the purpose of the data sharing, the users who will access the information, and the relationship of the parties. The agency privacy officer or designated agency counsel should consider including the following elements in a data sharing agreement or memoranda of understanding involving identifying information:

- A scope/statement of work that includes the purpose for which the information will be used, the specific groups or users who will have authorized access to the information, and the privacy and security protocols required to safeguard the information;
- A description of the specific data elements to be collected or shared, along with any applicable legal basis for the disclosure of such information;
- Restrictions on access to the information to authorized users for a permitted purpose in connection with the agreement;
- Limits on further disclosure to third parties without prior written authorization, or unless required by law, subpoena, or court order;
- Requirement of reasonable physical, technical, and procedural safeguards to protect the security of the information.

Sample language on privacy protection in developing data sharing agreements and memoranda of understanding is provided at **Appendix C**. Agency privacy officers or agency counsel may seek further guidance from the Chief Privacy Officer or Mayor's Office of Information Privacy in developing data sharing agreements and memoranda of understanding involving the sharing of identifying information.

6.2.3 Review by the Law Department

Unless otherwise determined by the Law Department, for agreements with City agencies involving the disclosure of identifying information by the City agency to external parties, agencies must consult the Law Department's Contracts Division to determine whether additional provisions, such as those regarding insurance, intellectual property and ownership, and indemnification are appropriate, and if so, for guidance on the required language for such provisions.

7.0 Training and Education Requirements

7.1 Citywide Privacy Protection Training

The Chief Privacy Officer, through the Mayor's Office of Information Privacy, will work with relevant agencies, including but not limited to representatives of the Citywide Privacy Protection Committee, the Department of Citywide Administrative Services, DoITT/Cyber Command, Law Department, and other relevant agencies to develop and implement citywide privacy protection training, adaptable by agencies, for use with appropriate employees and covered contractors and subcontractors on the requirements imposed by the Identifying Information Law and this Policy, along with a strategy or mechanism for tracking completion of the training by appropriate personnel. The Chief Privacy Officer, in consultation with such agencies and through other research, will explore various forms by which training may and will be implemented, including but not limited to online interactive modules, webinars, and privacy best practice guidance

[46] The Citywide Data Integration Initiative is managed by the Mayor's Office of Operations with technical facilitation provided by the DoITT.

materials, and will address other matters including frequency of training, mechanisms for updates, and issues relating to implementation of mandatory training for new hires.

7.2 Supplemental Agency Training

In addition to citywide training issued by the Chief Privacy Officer, agencies may develop agency specific privacy training as appropriate to the agency and the agency's covered contractors' and subcontractors' unique practices and needs. Such agency specific training must be consistent with the citywide privacy training implemented by the Chief Privacy Officer, and any applicable laws, regulations, or policies regarding the collection, retention, and disclosure of identifying or other information that is confidential pursuant to other law or regulation. For example, if the agency collects, retains, and discloses protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), as amended, supplemental training should touch on those requirements, as appropriate. Agency privacy officers should consult with their agency general counsel, the Chief Privacy Officer, or the City's Law Department as necessary, in the development of any supplemental agency training.

7.3 Agency implementation of Training Requirements

Agencies are responsible for identifying appropriate personnel and contractors and subcontractors who should receive privacy training. In determining whether personnel should be required to receive such training, agencies should consider, at a minimum, typical job responsibilities and functions and the level of access to identifying information those responsibilities and functions necessitate. Agencies should require periodic training of designated personnel, and covered contractors and subcontractors as necessary to remain current with privacy and confidentiality requirements relevant to their job responsibilities and functions.

8.0 Protocol for Receiving and Investigating Complaints for Violations of the Identifying Information Law

In accordance with Admin. Code § 23-1203(9), the Chief Privacy Officer must establish a mechanism for accepting and investigating complaints for violations of the Identifying Information Law. Agency privacy officers shall collaborate with the Chief Privacy Officer on compliance with this requirement, following the protocols set forth in **Section 8.2** below.

8.1 Violations

A violation of the Identifying Information Law occurs where identifying information is collected or disclosed by a City agency employee, or covered contractor or subcontractor in a manner not consistent with the requirements of the Identifying Information Law. Except under exigent circumstances or where a law or treaty precludes compliance, an agency that is required to comply with the Identifying Information Law that has been advised by the Chief Privacy Officer of its compliance obligations under the Identifying Information Law but has continued to collect, disclose, or retain identifying information in a manner inconsistent with the requirements of the Identifying Information Law despite such notification by the Chief Privacy Officer shall be deemed in violation of the Identifying Information Law. Such violations will be reported by the Chief Privacy Officer in accordance with Admin. Code § 23-1202(c)(4).

8.2 Receiving and Investigating Complaints

City agencies must adopt written protocols for receiving and investigating complaints[47] under the Identifying Information Law which, at a minimum:

[47] For purposes of this section, "complaint" refers to a notification regarding a suspected or known violation of the Identifying Information Law. The law does not create a private right of action.

- Designates the agency privacy officer, or other appropriate individual, as the primary point of contact for receiving and investigating such complaints, and gathering relevant facts surrounding the complaint or violation;
- Sets forth the channel of communication for making complaints;
- Requires the agency privacy officer to promptly investigate the potential or known violation;
- Requires the agency privacy officer, or other appropriate individual, to coordinate with internal legal, program, technical, or other staff to engage in fact finding relevant to the complaint;
- Requires assessment of potential implications arising under any other applicable laws, regulations, or policies;
- Requires the agency privacy officer, once aware of a disclosure in violation of the Identifying Information Law or this Policy, to notify the Chief Privacy Officer of such disclosure as soon as practicable;[48] and
- Provides for other relevant City offices to be engaged, including the Chief Privacy Officer, the Law Department, Cyber Command, DoITT, and others deemed appropriate by the agency or such officials to assist in the investigation and advise on a response, depending on the factual and legal circumstances surrounding a potential or known violation.

Agency protocol for receiving and investigating complaints must be implemented in a manner that is consistent with any applicable legal, regulatory, or policy requirements. Mechanisms for accepting complaints must be made known and available to agency personnel, and covered contractors and subcontractors. Agencies should contact the Chief Privacy Officer as necessary for guidance relating to this section.

8.3 Notification Requirements

Agencies must make reasonable efforts to notify individuals in writing when their identifying information has been accessed or disclosed in violation of the Identifying Information Law to third parties when:

(1) Required by law or regulation;
(2) There is potential risk of harm to the individual, including but not limited to a risk of harm that may be physical, financial, reputational, or other harms dependent upon any protected status of an individual, status as a victim or witness to a crime, or similar considerations; or
(3) In other circumstances where no legal obligation exists, where the agency determines, in consultation with the Chief Privacy Officer and City's Law Department, that notification to such individuals should occur.[49]

In determining whether notification must be made under this section, Agency Privacy Officers should consult with appropriate agency counsel and, as necessary, the Chief Privacy Officer.

Where a disclosure of identifying information prohibited by law or regulation has occurred, the agency must comply with the applicable legal notification requirements. Such prohibited disclosures include, but are not limited to disclosures of identifying information that may have occurred as part of a "breach of security" as defined by Admin. Code § 10-501, in accordance with the procedures set forth in Admin. Code § 10-502, as appropriate.

[48] See Admin. Code § 23-1202(c)(4).
[49] The Chief Privacy Officer and Law Department will further coordinate with other relevant City officials as necessary to determine whether notification should occur, such as the DoITT and Cyber Command.

Mayor's Office of Information Privacy

Page Intentionally Blank

Mayor's Office of Information Privacy

Appendix A – List of City Entities Exempt from the Identifying Information Law

The New York City Law Department has advised that the Identifying Information Law does not apply to the following City-related agencies and entities:

- Board of Elections
- Brooklyn Navy Yard Development Corporation
- Brooklyn Public Library
- City University of New York
- Department of Education
- District Attorney Bronx County
- District Attorney Kings County
- District Attorney New York County
- District Attorney Queens County
- District Attorney Richmond County
- Economic Development Corporation
- Housing Development Corporation
- Hudson Yards Development Corporation
- New York City Housing Authority
- New York Public Library
- NYC & Company, Inc.
- NYC Health + Hospitals
- Public Administrator Bronx County
- Public Administrator Kings County
- Public Administrator New York County
- Public Administrator Queens County
- Public Administrator Richmond County
- Queens Public Library
- School Construction Authority
- The Trust for Governors Island

Mayor's Office of Information Privacy

Page Intentionally Blank

Mayor's Office of Information Privacy

Appendix B – Identifying Information Law Rider

Identifying Information Rider

(To supplement the City Standard Human Services Contract,
the Discretionary Fund Contract for human services contracts less than $100,000,
other human services contracts and other contracts designated by the Chief Privacy Officer)

Section 1.01 Background.

Local Laws 245 and 247 of 2017 (codified at New York City Charter ("Charter") Section 8 subdivision (h) and the Administrative Code of the City of New York ("Admin. Code") Sections 23-1201 to -1205) are effective June 15, 2018. Such laws apply to human services contracts and other contracts designated by the City Chief Privacy Officer that involve the collection, retention, or disclosure of "Identifying Information" in connection with services provided under a City contract. Accordingly, in connection with the services provided under this Agreement, Contractor may collect, retain, and disclose Identifying Information only in accordance with the requirements of this Identifying Information Rider, the policies and protocols adopted pursuant to Admin. Code Sections 23-1201 to -1205, the other provisions of this Agreement and as otherwise required by law.

Section 1.02 Definitions.

A. "Agency" means the City agency or office through which the City has entered into this Agreement.

B. "Agency Privacy Officer" means the person designated to exercise functions under Admin. Code Sections 23-1201 to -1205 by the Agency through which the City is a party to this Agreement.

C. "City Chief Privacy Officer" means the person designated by the Mayor pursuant to Charter Section 8 subdivision (h) as the City's Chief Privacy Officer or such person's designee.

D. "Exigent Circumstances" means circumstances where collection or disclosure is urgently necessary, such that procedures that would otherwise be required cannot be followed.

E. "Identifying Information" means any information provided by the City to Contractor or obtained by Contractor in connection with this Agreement that may be used on its own or with other information to identify or locate an individual. Identifying Information includes, but is not limited to: name, sexual orientation, gender identity, race, marital or partnership status, status as a victim of domestic violence or sexual assault, status as a crime victim or witness, citizenship or immigration status, eligibility for or receipt of public assistance or city services, all information obtained from an individual's income tax records, an individual's Social Security number, information obtained from any surveillance system operated by, for the benefit of, or at the direction of the New York City Police Department, motor vehicle information or license plate number, biometrics such as fingerprints and photographs, languages spoken, religion, nationality, country of

origin, place of birth, date of birth, arrest record or criminal conviction, employment status, employer information, current and previous home and work addresses, contact information such as phone number and email address, information concerning social media accounts, date and/or time of release from the custody of the Administration for Children's Services, the Department of Correction, or the New York City Police Department, any scheduled court appearances, any scheduled appointments with the City, the Contractor or its subcontractor that provides human services or other services designated by the City Chief Privacy Officer, and any other category of information designated by the City Chief Privacy Officer.

Section 1.03 Collection.

Absent Exigent Circumstances, Contractor shall not collect Identifying Information unless such collection (a) has been approved by the Agency Privacy Officer or the City Chief Privacy Officer and the collection of such Identifying Information is in furtherance of Contractor's obligations under this Agreement; (b) is required by law or treaty; (c) is required by the New York City Police Department in connection with a criminal investigation; or (d) is required by a City agency in connection with the welfare of a minor or other individual who is not legally competent.

Section 1.04 Disclosure.

A. Absent Exigent Circumstances, Contractor shall not disclose Identifying Information unless such disclosure (a) has been authorized in writing by the individual to whom such information pertains or, if such individual is a minor or is otherwise not legally competent, by such individual's parent, legal guardian, or other person with legal authority to consent on behalf of the individual; (b) has been approved by the Agency Privacy Officer or the City Chief Privacy Officer and the disclosure of such Identifying Information is in furtherance of Contractor's obligations under this Agreement; (c) is required by law or treaty; (d) is required by the New York City Police Department in connection with a criminal investigation; or (e) is required by a City agency in connection with the welfare of a minor or other individual who is not legally competent.

B. If Contractor discloses an individual's Identifying Information in violation of this Rider, Contractor shall notify the Agency Privacy Officer. In addition, if such disclosure requires notification to the affected individual(s) pursuant to the policies and protocols promulgated by the City Chief Privacy Officer under subdivision 6 of Section 23-1203, in the discretion of the Agency Privacy Officer Contractor shall either (i) make reasonable efforts to notify such individual(s) in writing of the Identifying Information disclosed and to whom it was disclosed as soon as practicable or (ii) cooperate with the Agency's efforts to notify such individual(s) in writing. The City shall have the right to withhold further payments under this Agreement for the purpose of set-off in sufficient sums to cover the costs of notifications and/or other actions mandated by any law, administrative or judicial order, or the City Chief Privacy Officer to address the disclosure, and including any fines or disallowances

imposed by the State or federal government as a result of the disclosure. The City shall also have the right to withhold further payments hereunder for the purpose of set-off in sufficient sums to cover the costs of credit monitoring services for the victims of such a disclosure by a national credit reporting agency, and/or any other commercially reasonable preventive measure. The Agency shall provide Contractor with written notice and an opportunity to comment on such measures prior to implementation. Alternatively, at the City's discretion, or if monies remaining to be earned or paid under this Agreement are insufficient to cover the costs detailed above, Contractor shall pay directly for the costs, detailed above, if any.

C. Section 1.04(B) shall not require any notification that would violate any law or interfere with an investigation or otherwise compromise public safety pursuant to subdivision e of Section 23-1204.

Section 1.05 Exigent Circumstances.

In the event Contractor collects or discloses Identifying Information due to Exigent Circumstances, with no other basis for collection or disclosure under subdivisions b or c of Section 23-1202, Contractor shall send to the Agency Privacy Officer information about such collection or request and disclosure, along with an explanation of why such Exigent Circumstances existed, as soon as practicable after such collection or disclosure. This section shall not require any such notification for collection or disclosure of Identifying Information that: (a) is required by the New York City Police Department in connection with an open criminal investigation; (b) is required by a City agency in connection with an open investigation concerning the welfare of a minor or other individual who is not legally competent; or (c) occurs in the normal course of performing Contractor's obligations under this Agreement and is in furtherance of law enforcement or public health or safety powers of the Agency under Exigent Circumstances.

Section 1.06 Retention.

Contractor shall retain Identifying Information as required by law or as otherwise necessary in furtherance of this Agreement, or as otherwise approved by the Agency Privacy Officer or the City Chief Privacy Officer.

Section 1.07 Reporting.

Contractor shall provide the Agency with reports as requested by the Agency Privacy Officer or City Chief Privacy Officer regarding the collection, retention, and disclosure of Identifying Information by Contractor. Each such report shall include information concerning Identifying Information collected, retained, and disclosed, including: (a) the types of Identifying Information collected, retained, or disclosed; (b) the types of collections and disclosures classified as "routine" and any collections or disclosures approved by the Agency Privacy Officer or City Chief Privacy Officer; and (c) any other related information that may be reasonably required by the Agency Privacy Officer or City Chief Privacy Officer.

Section 1.08 Coordination with Agency Privacy Officer.

The Agency may assign powers and duties of the Agency Privacy Officer to Contractor for purposes of this Agreement. In such event, Contractor shall exercise those powers and duties in accordance with applicable law in relation to the Agreement, and shall comply with reasonable directions of the Agency Privacy Officer and City Chief Privacy Officer concerning coordination and reporting.

Section 1.09 Conflicts with Provisions Governing Records, Audits, Reports and Investigations.

To the extent allowed by law, the provisions of this Rider shall control if there is a conflict between any of the provisions of this Rider and, as applicable, either (i) Article 5 of Appendix A (General Provisions Governing Contracts for Consultants, Professional, Technical, Human, and Client Services); (ii) if the value of this Agreement is $100,000 or less and the Agreement is funded by City Council Discretionary Funds, Article 7(E) and Rider 1, Article 1 of the Agreement; or (iii) if neither (i) nor (ii) apply, the Investigations Clause, and other provisions concerning records retention, inspections, audits, and reports designated elsewhere in the Agreement. The provisions of this Rider do not replace or supersede any other obligations or requirements of this Agreement.

Section 1.10 Subcontracts.

A. Contractor shall include this Rider in all subcontracts to provide human services or other services designated in the policies and protocols of the City Chief Privacy Officer.
B. Contractor agrees that it is fully responsible to the Agency for the compliance with this Rider by its subcontractors that provide human services or other services designated by the City Chief Privacy Officer.

Section 1.11 Disclosures of Identifying Information to Third Parties.

Contractor shall comply with the City Chief Privacy Officer's policies and protocols concerning requirements for a written agreement governing the disclosure of Identifying Information to a third party.

Mayor's Office of Information Privacy

Appendix C – Sample Privacy Protection and Confidentiality Language for Use in Developing Data Sharing Agreements

Instructions: *The sample language in this document is provided as guidance only for purposes of drafting provisions relating to privacy and security protection in Memoranda of Understanding or Data Sharing Agreements involving the collection or disclosure of identifying information between and among City agencies, and/or between City agencies and external entities. It is not intended as an exhaustive compilation of all provisions required for the agreement. Agency counsel can and should adapt and modify the below template language as appropriate to the specific purpose or project for which the agreement is necessary.*

Note also the following additional information:

- *For agreements between City agencies that also involve external parties, agencies should consult with the New York City Law Department to determine the need for additional provisions, including but not limited to insurance and indemnification, unless otherwise determined by the Law Department.*
- *The term "Identifying Information" is used to describe the data or information to be collected or disclosed pursuant to the agreement; a different term can be used to appropriately describe such data or information (e.g., "Data," "Confidential Information," etc.).*
- *Certain disclosures of identifying information may warrant additional data retention and data destruction requirements. Agency counsel should contact the agency's general counsel or as necessary, consult with the Chief Privacy Officer or City's Law Department as to whether or not such additional provisions should be included.*

A. Access to Identifying Information in connection with this Agreement is restricted to "Authorized Users" for a "Permitted Use." For purposes of this Agreement, an Authorized User and "Permitted Use" shall include, respectively, only those of Recipient's employees and agents whose access to or use of the **Identifying Information** is necessary to carry out Recipient's obligations under this MOU and Scope of Work, or as required by law.

B. Other than as provided for under this Agreement, Recipient shall not disclose **Identifying Information** to any third parties nor make use of such information for the benefit of another, nor shall Recipient publish, sell, license, distribute, or otherwise reveal the **Identifying Information** without the prior written authorization of the individual or prior written approval of the Agency. All third party requests for **Identifying Information** received by Recipient shall be promptly communicated to the relevant agency upon receipt and handled by the Agency Privacy Officer, unless otherwise required by law.

C. No Identifying Information shall be disclosed by Recipient without either (i) prior written consent of the affected individual; or (ii) the prior express authorization of the Agency, *provided, however,* that in the event that disclosure of the **Identifying Information** is required by Recipient under the provision of any subpoena, law or court order, Recipient will: (a) as soon as practicable, but in no event later than [**enter the appropriate time range; recommended to be no less than three (3) but no more than five (5)]** business days from receipt of said subpoena, court order or law requiring such disclosure, notify the Agency in order to allow the relevant agency to seek a protective order as appropriate; and (b) disclose the **Identifying Information** only to the extent allowed under a protective order, if any, or as necessary to comply with the subpoena, law or court order.

D. Recipient shall ensure that reasonable physical, technological, and procedural safeguards are in place to protect the security of **Identifying Information**, including but not limited to ensuring that its personnel understand their obligations under this Agreement and applicable laws and regulations. Recipient shall protect against any anticipated hazards or threats to the integrity or security of the **Identifying Information** and any unauthorized access to or disclosure of such information, and shall take reasonable measures to prevent any other action that could result in harm to the City and the individuals whose **Identifying Information** is held in Recipient's custody. Recipient shall

comply with the City's IT security standards and requirements, set forth by the New York City Department of Information Technology and Telecommunications (DoITT), as they may be modified from time to time.

> ***Note*****:** *Agencies might consider describing here certain specific types of safeguards based on the type of third party and agreement. Agencies should be mindful of the capacity such third party has to implement certain safeguards and the evolving nature of technology over time. Agencies should consult with the Department of Information Technology and Telecommunications as necessary to determine necessary and appropriate safeguards.*

E. **REPORTING.** Recipient shall immediately notify the Agency in writing if Recipient suspects or learns of any unauthorized use or disclosure of the **Identifying Information** by its personnel or any third party who gained unauthorized access to such information, so that the Agency can investigate the incident, and in such circumstances, Recipient shall take all reasonably necessary steps to prevent or mitigate damages related thereto, including but not limited to providing or assisting in providing any affected individual(s) with notice as determined to be necessary. Recipient's notice to the agency shall include a description of the nature of the unauthorized use or disclosure, the **Identifying Information** that may have been disclosed, the names and/or the affiliations of the parties (if known) who gained access to data without authorization, and a description of the steps taken, if any, to mitigate the effects of such unauthorized use or disclosure, in accordance with all relevant laws and regulations. Such notice shall be provided to:

FOR [Agency Name]:
[**Name**]
[**Title**]
[**Address**]
[**Email**]

FOR [Agency Name]:
[**Name**]
[**Title**]
[**Address**]
[**Email**]

Mayor's Office of Information Privacy

Appendix D – Table Cross-Referencing CPO Policy with Required Provisions under Section 23-1203 of the Administrative Code

The following table lists and cross references requirements for the Chief Privacy Officer's ("CPO's") Policies and Protocols under N.Y.C. Admin. Code § 23-1203 with the implementing sections in the CPO Policies and Protocols.

#	Requirements under Admin. Code § 23-1203	Implementing sections in CPO Policies and Protocols
1	Require that identifying information is anonymized where appropriate in accordance with the purpose or mission of a City agency.	• 5.6.1 Anonymization
2	Require the privacy officer of each City agency to issue guidance to City agency employees, contractors, and subcontractors regarding such agency's collection, retention, and disclosure of identifying information.	• 4.2.1 Agency Privacy Protection Policies and Guidance
3	Require any City agency disclosing identifying information to a third party when such a disclosure is not classified as routine pursuant to section 23-1202 to enter into an agreement ensuring that the anticipated use and any potential future use of such information by such third party occurs only in a manner consistent with this chapter unless: (i) such disclosure is made under exigent circumstances, or (ii) such an agreement would not further the purposes of this chapter due to the absence of circumstances in which such disclosure would unduly compromise an important privacy interest.	• 6.2.1 When an Agreement is Required
4	Describe disclosures of identifying information to third parties when such a disclosure is classified as routine pursuant to section 23-1202 for which, because of the nature or extent of such disclosures or because of the nature of the relationship between the City agency and third party, such disclosing agency is required to enter into an agreement with such third party requiring that the anticipated use and any potential future use of such information by such third party occurs only in a manner consistent with this chapter.	• 6.2.1 When an Agreement is Required
5	Describe disclosures of identifying information that are not to be treated as routine pursuant to section 23-1202, as determined by the nature and extent of such disclosures, and require an additional level of review and approval by the privacy officer of such agency or the contractor or subcontractor before such disclosures are made.	• 5.2.1 Considerations in Determining Whether a Collection or Disclosure is "Routine" or "Non-Routine"
6	Describe circumstances when disclosure of an individual's identifying information to third parties in violation of this chapter would, in light of the nature, extent, and foreseeable adverse consequences of such disclosure, require the disclosing City agency, contractor, or subcontractor to make reasonable efforts to notify the affected individual as soon as possible;	• 8.3 Notification Requirements
7	Establish standard contract provisions, or required elements of such provisions, related to the protection of identifying information.	• 6.2.2 Elements of Data Sharing Agreements • Appendix C (Identifying Information Law Rider)
8	Require the privacy officer of each City agency to arrange for dissemination of information to agency employees, contractors, and subcontractors and develop a plan for compliance with this chapter and any policies and protocols developed under this chapter.	• 4.2.1 Agency Privacy Protection Policies and Guidance
9	Establish a mechanism for accepting and investigating complaints for violations of this chapter.	• 8.2 Receiving and Investigating Complaints

Page Intentionally Blank