Mayor's Office of Information Privacy

LAURA NEGRÓN
CHIEF PRIVACY OFFICER

Citywide Privacy Protection Policies and Protocols

February 24, 2021

Page Intentionally Blank

Mayor's Office of Information Privacy

VERSION CONTROL

Version	Description of Change	Approver	Date
2.0	Introduced guidance tips, made clarifications, and added sub-sections Expanded NYS Freedom of Information Law and NYC Open Data Law guidance Designated taxpayer ID number, palm and handprints, retina and iris patterns, facial geometry, gait or movement patterns, voiceprints, and DNA sequences as new types of identifying information and updated Identifying Information Table Enhanced guidance relating to requests from oversight agencies Designated technology services involving sensitive identifying information and certain outreach contracts and subcontracts as subject to the Identifying Information Law Enhanced guidance relating to contracts and "routine" designations Introduced recommendation for agencies to publish their privacy protocols to agency websites Updated and added appendices, including new Privacy Protection Rider	Laura Negrón Chief Privacy Officer, City of New York	2/24/2021
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

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.[2]

1.3 Applicability

This Policy applies to all City agencies, except those exempt from the requirements of the Identifying Information Law[3] (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[4] and other services designated by the Chief Privacy Officer ("covered contractors and subcontractors") must comply with this Policy.[5]

The agency privacy officer[6] 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] 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 Identifying Information 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] Exempt agencies may and are strongly encouraged to comply with the mandates of the Identifying Information Law and this Policy.
[4] "Human services" has the meaning set forth in Admin. Code § 6-129(c).
[5] Refer to **Section 6.0** of this Policy on Contracts.
[6] 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.

1.4 Modification

This Policy 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 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.[7]

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,[8] 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 and related guidance.

> ➢ **Guidance Tip**: Developing relationships with other agency stakeholders, such as records access officers, chief information security officers, and agency chief contracting officers, can help agency privacy officers stay up to date on relevant agency and citywide developments. The Chief Privacy Officer may also, in coordination with the NYC Cyber Command and the New York City Department of Information Technology and Telecommunications, disseminate relevant information technology and security policies to agency privacy officers.

[7] This Policy incorporates revisions based on recommendations made by the Citywide Privacy Protection Committee in 2020.
[8] 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.

1.5.3 Citywide Information Technology and Security Policies and Standards

The Citywide Cybersecurity Program Policies & Standards[9] and Citywide Technology Policies and Guidelines,[10] 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"). 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:

- Agency Incident Response Plan
- Citywide Cloud Policy[11]
- Citywide Incident Response Policy
- Data Classification Standard
- Citywide Information Management Standard
- Digital Media Re-Use and Disposal Policy
- Encryption Security Policy
- Encryption Standards
- Mobile Computing Device Security Policy
- User Responsibilities Security Policy
- Portable Data Security Policy

Identifying information that is determined to be "sensitive identifying information," as such term is defined in this Policy,[12] should be classified as Restricted information pursuant to the Data Classification Standard and 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. See **Sections 3.2.5** and **6.2.1** for additional information on protecting sensitive identifying information.

[9] Available at http://cityshare.nycnet/portal/site/cityshare/menuitem.60a2a41bbe6db8deeb83af10ec9089a0/.
[10] Available at http://cityshare.nycnet/portal/site/cityshare/menuitem.82865db917088750fc5cd710ec9089a0/. The cybersecurity requirements for vendors and contractors are available at https://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page.
[11] The Citywide Cloud Policy requires that City agencies and entities submit any plans to use cloud services to DoITT for review so that appropriate security, legal, and operational measures are considered and approved (*see* http://cityshare.nycnet/html/service-offering/html/professional/cloud-review.shtml for DoITT's cloud review procedure and a link to the Citywide Cloud Policy).
[12] *See* **Section 3.2.5**.

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;[13] 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. Refer to **Section 6.0** for additional guidance on incorporating privacy terms and various privacy and security-related attachments into agreements.

> ➢ **Guidance Tip**: The Chief Privacy Officer, in collaboration with Cyber Command and DoITT, will help facilitate distribution of relevant guidance about data security to agency privacy officers. Agency privacy officers can also raise questions about privacy and data security directly to the Chief Privacy Officer at PrivacyOfficer@cityhall.nyc.gov or at scheduled agency privacy officer convenings.

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.[14] Agency compliance with Mayoral Directive 2015-3,[15] 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 retaining 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"),[16] issued as City policy in April 2017 by the First Deputy Mayor,[17] which set forth a factual and legal assessment process that agencies must follow when handling a request from a third party for City information, including but not limited to a request that may contain identifying information. Agencies must either adopt the Model Protocols in their entirety or develop and adopt a comparable protocol.[18]

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

[13] Relevant agency-specific policies may include Acceptable Use Policies, Acceptable Email Usage Policies, IT and Equipment Policies, and Remote Access Policies. These policies 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.
[14] *See* Admin. Code § 23-1202(e).
[15] Available at https://www1.nyc.gov/assets/records/pdf/Mayoral%20Directive%20No.%202015-3.pdf.
[16] The Model Protocols are consistent with the requirements of the Identifying Information Law and this Policy, each of which requires agency review of relevant laws and facts before disclosures of identifying information can be made.
[17] The Model Protocols are on file with the Mayor's Office of Information Privacy.
[18] Email directive on file with the Mayor's Office of Information Privacy.

domestic violence, status as a victim of sexual assault, status as a crime witness, receipt of public assistance, or immigration status [and] all information contained in any individual's income tax records." Executive Order 41 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[19]

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 government records, and establishes a duty for City agencies to disclose such records in response to a request unless an exemption applies.[20] Such records may include identifying information. When FOIL, a state law, requires an agency to disclose identifying information, the agency should disclose it[21] and will not need to comply with the requirements of the Identifying Information Law with respect to that disclosure. Agency privacy officers may document such disclosures as "authorized" because the disclosure is required by law.[22]

If an exemption to the disclosure requirements under FOIL applies, such as where the disclosure would constitute an unwarranted invasion of personal privacy, but the agency is considering whether to voluntarily disclose some or all of the requested identifying information, the agency will need to comply with the Identifying Information Law. Specifically, in order to disclose the information, the agency privacy officer will need to determine that the disclosure furthers the purpose or mission of the agency.[23]

1.6.1.1 Publishing FOIL Request Titles on the Open Records Portal

Individuals may submit FOIL requests by contacting a City agency directly, or by submitting a request through the City's FOIL portal ("OpenRecords Portal" or "Portal"), which is managed by DORIS.[24] The OpenRecords Portal displays certain information about every FOIL request placed on the Portal, including the title created for it by the member of the public who submitted the request.[25] The request title may contain identifying information. When an agency receives a FOIL request via the OpenRecords Portal, the agency should determine whether the title of the request contains any identifying

[19] For additional guidance on the relationship between the Identifying Information Law and other laws and regulations, contact relevant agency counsel, the Chief Privacy Officer, or the Law Department, as needed.
[20] *See* Public Officers Law Article 6. "All government records are [] presumptively open for public inspection and copying unless they fall within one of the enumerated exemptions of Public Officers Law § 87 (2)." *Matter of Gould v New York City Police Dept.*, 89 N.Y.2d 267, 274-75 (1996).
[21] FOIL, a state law, takes precedence over the Identifying Information Law, a local law.
[22] *See* Admin. Code § 23-1202(c)(1)(c).
[23] *See* Admin. Code § 23-1202(c)(1)(b).
[24] Agencies may also choose to use the OpenRecords Portal to publish information about FOIL requests they receive directly. Any member of the public may access the information published on the OpenRecords Portal.
[25] It also includes the date of the request, status updates on the processing of the request, and, if the agency so chooses, the records released in response to the request.

information that should not be publicly disclosed on the Portal (such as Social Security numbers).[26] To give records access officers time to make this determination in consultation with their agency privacy officer, the system is programmed to temporarily withhold FOIL request titles from publication on the OpenRecords Portal for five business days. This delay purposefully coincides with the FOIL "acknowledgement period."[27] Therefore, the determination as to whether or not any identifying information contained in the FOIL request title should be redacted must be made within this five-day period.

- **Guidance Tip**: Each agency subject to FOIL has a records access officer who is responsible for responding to FOIL requests. Refer to **Section 4.1.1.1** for information relating to the records access officer.
- **Guidance Tip**: Records access officers should coordinate with their agency privacy officer on the agency's response to requests for disclosure of identifying information made in a FOIL request where disclosure is not mandatory under FOIL, and a FOIL exemption is available but the agency is considering whether to disclose the information voluntarily.[28]

1.6.2 Open Data Law

Local Law 11 of 2012 (the "Open Data Law"), as amended,[29] mandates that all "public data sets" be made accessible on a single web portal ("Open Data Portal"). "Public data set" means "a comprehensive collection of interrelated data that is available for inspection by the public in accordance with any provision of law and is maintained on a computer system by, or on behalf of, an agency."[30] Whether identifying information constitutes a "public data set" is a legal determination.

Information that any law restricts from disclosure is not considered a public data set.[31] Seven types of data are excluded from the definition of "public data set," including "any portion of such data set to which an agency may deny access pursuant to the public officers law or any other provision of a federal or state law, rule or regulation or local law."[32] The Identifying Information Law is such a local law.

Open data coordinators should consult with their agency privacy officers to determine whether the agency's public data sets include identifying information before such data is made publicly available. If the data set contains identifying information, the open data coordinator and agency privacy officer should collaborate so that any publication of identifying information on the Open Data Portal complies with the requirements of the Identifying Information Law, this Policy, and any other applicable laws and regulations.

- **Guidance Tip**: The Open Data Policy and Technical Standards Manual contains additional guidance on identifying information, privacy, and the Open Data Law.[33]

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 to 10-504, set forth requirements for City agencies to follow in the event that an agency disclosure of "personal identifying information"[34] constitutes a

[26] The OpenRecords Portal is available at https://www1.nyc.gov/site/records/nyc-government-records/open-records-portal.page.
[27] N.Y. Pub. O. Law § 89(3)(a) grants entities subject to FOIL five business days to acknowledge receipt of a FOIL request.
[28] *See* "Guidance on the City's Identifying Information Law in relation to Open Data" (on file with the Mayor's Office of Information Privacy) for additional guidance on this subject.
[29] *See* Admin Code § 23-501 *et seq*.
[30] *See* Admin. Code § 23-501(g).
[31] *Id.*
[32] *Id.*
[33] The Open Data Policy and Technical Standards Manual is available at https://opendata.cityofnewyork.us/tsm/. If it is not accessible, please contact the NYC Open Data team at https://opendata.cityofnewyork.us/engage/.

"breach of security."[35] Where identifying information meets the definition of personal identifying information[36] 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.

1.6.4 Local Law 30 of 2017

Pursuant to Local Law 30 of 2017, agencies providing direct public services (meaning, services administered by an agency directly to program beneficiaries, participants, or applicants) or emergency services must translate documents containing information about public services that they most commonly distribute. Per the Identifying Information Law, "languages spoken" is a type of identifying information. Agencies that are collecting or disclosing such information from members of the public to inform their language access strategies or comply with the mandates of Local Law 30 should include, in their biennial agency reports, "languages spoken" as a type of identifying information that the agency collects or discloses.

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.

---

[34] *See* Admin. Code § 10-501(a).
[35] *See* Admin. Code § 10-501(b).
[36] Note that "personal identifying information" as defined in Admin. Code § 10-501 is a subset of "identifying information" as defined in Admin. Code § 23-1201.

	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 their 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 individuals' 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.

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.[37] The Identifying Information Law enumerates certain types of information that are covered by this definition, and authorizes the Chief Privacy Officer to designate additional types of information to be covered.

The enumerated types of identifying information below represent a non-exhaustive list of information that constitutes identifying information. Agencies should interpret the definition of identifying information broadly, so that any information that alone or in combination with other information can identify or locate an individual is afforded appropriate privacy protection.

[37] *See* Admin. Code § 23-1201.

Enumerated Types of Identifying Information:	
<u>Personal Information</u> Name Social Security number (full or last 4 digits)* Taxpayer ID number (full or last 4 digits)*	**<u>Work-Related Information</u>** Employer information Employment address
<u>Biometric Information</u> Fingerprints Photographs Palm and handprints* Retina and iris patterns* Facial geometry* Gait or movement patterns* Voiceprints* DNA sequences*	**<u>Government Program Information</u>** Any scheduled appointments with any employee, contractor, or subcontractor Any scheduled court appearances Eligibility for or receipt of public assistance or City services Income tax information Motor vehicle information
<u>Contact Information</u> Current and/or previous home addresses Email address Phone number	
<u>Demographic Information</u> Country of origin Date of birth* Gender identity Languages spoken Marital or partnership status Nationality Race Religion Sexual orientation	**<u>Law Enforcement Information</u>** Arrest record or criminal conviction Date and/or time of release from custody of ACS, DOC, or NYPD Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD
<u>Status Information</u> Citizenship or immigration status Employment status Status as victim of domestic violence or sexual assault Status as crime victim or witness *types of Identifying Information designated by the Chief Privacy Officer	**<u>Technology-Related Information</u>** Device identifier 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***** Internet protocol (IP) address***** Social media account information

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)
- Taxpayer ID 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
- Palm and handprints
- Retina and iris patterns
- Facial geometry
- Gait or movement patterns
- Voiceprints
- DNA sequences

> ➢ **Guidance Tip**: Agency privacy officers must update relevant agency compliance documentation, such as their records of routine and non-routine designations, to include any additional types of identifying information designated by the Chief Privacy Officer, if the agency collects, retains, or discloses such information.

3.1.2 Guidance in Determining when Other Information Constitutes Identifying Information

Unless information has been designated as a type of "identifying information" under Admin. Code § 23-1201 or by the Chief Privacy Officer, determining whether or not it 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 fewer 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 or 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, pseudonymization, redaction, encryption, masking, and hashing. See **Section 5.6.1** for additional guidance about anonymization.

3.2.2 Collection

"Collection" shall be understood to mean the act of directly or indirectly receiving, retrieving, extracting, 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 applies 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 applies only to a very limited number of agencies, such as DoITT.

3.2.4 Exigent Circumstances

"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.

Information designated as "sensitive identifying information" should be classified as "Restricted" information pursuant to the Citywide Cybersecurity Program Policies and Standards,[38] and handled in accordance with the applicable security protection requirements, whether in physical or electronic format. Sensitive identifying information must only be stored in secure databases or on secure file servers using the appropriate encryption protocol set forth in the Citywide Encryption Standard. It should not be stored or transmitted across any communication mechanism unless it is protected using City-approved data encryption technology or by other secure means, such as a secure web service.

Refer to **Section 3.1** for the definition of "identifying information," **Section 5.5.1** for requirements for requests and proposals involving sensitive identifying information, and **Appendix G** for guidance on protecting sensitive identifying information in relevant provisions of contracts.

[38] Available at http://cityshare.nycnet/portal/site/cityshare/menuitem.60a2a41bbe6db8deeb83af10ec9089a0/.

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). These terms shall be understood to have the following meanings:

"Requests" for identifying information shall be understood to mean requests for the release or production of identifying information by a third party, such as but not limited to: press or 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 the Open Data Law.

"Proposals" for identifying information shall be understood to 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 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.

> ➢ **Guidance Tip**: The Chief Privacy Officer and the Mayor's Office of Information Privacy provide new agency privacy officers with up-to-date training and guidance related to the mandates of the Identifying Information Law as needed to help them perform their duties effectively.

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.[39] Refer to **Section 1.6.1** on the relationship of FOIL to the Identifying Information Law.

[39] *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.[40] If the agency makes such a designation, the covered contractor or subcontractor will be responsible for 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[41] 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.[42] 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.

- **Guidance Tip**: Agency privacy officers should periodically meet with their agencies' technical staff, including chief information security officers, given the interface between privacy protection and data security and technology services. The Agency Privacy Officer Toolkit[43] will be updated by the Mayor's Office of Information Privacy with additional guidance highlighting the importance of this collaboration.

- **Guidance Tip**: Agency privacy officers may benefit from consulting with the Chief Privacy Officer or other agency privacy officers, particularly on matters that affect more than one agency, including citywide initiatives. Agency privacy officers can ask the Chief Privacy Officer to convene working groups to facilitate interagency collaboration. The Chief Privacy Officer will, for example, convene a working group to examine privacy considerations relating to identifying information maintained in citywide administrative databases, such as the Financial Management System (FMS), NYCAPS, and CityTime. For new databases being considered by the City or any agency, this working group or a subgroup thereof could be leveraged to develop protocols or recommended best practices to protect privacy.

[40] *See* Admin. Code § 23-1202(g).
[41] *See* Admin. Code § 23-1205.
[42] *See* Admin. Code § 23-1203(2).
[43] Available at https://www1.nyc.gov/site/moip/reports/reports.page.

4.2.2 Agency Compliance Plan

Agency privacy officers should develop a plan for compliance with the Identifying Information Law and this Policy.[44] The Chief Privacy Officer has issued model protocols and policies for agencies and offices to help guide agency privacy officers in Identifying Information Law compliance. Model protocols and policies are designed to help support baseline citywide compliance with the Identifying Information Law, and provide agency privacy officers with tools that promote customized and comprehensive reporting.

> ➢ **Guidance Tip**: The Chief Privacy Officer has issued baseline model compliance plans and guidance as part of the Agency Privacy Officer Toolkit which agencies can adopt or adapt to fulfill the requirements of this section.[45] The Toolkit contains tools for agency privacy officers to assess and improve their internal compliance processes. The Toolkit is a shared document and agency privacy officers are encouraged to contribute their respective agencies' forms and compliance practices.

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."[46] 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.

> ➢ **Guidance Tip**: Although agency privacy officers may consult with the Chief Privacy Officer on whether or not a collection or disclosure of identifying information should be designated as "routine," the agency privacy officer is authorized under the Identifying Information Law to make these determinations, which are largely informed by the mission, purpose, internal functions, and structure of the agency.

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.[47] 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.

Unless exigent circumstances exist, agencies must obtain approval from their agency privacy officers for projects involving the collection or disclosure of identifying information that have not previously been designated as "routine."

Note that an agency privacy officer may designate additional types of collections and disclosures as "routine" at any time, and may also approve collections and disclosures that have not been so designated on a case-by-case basis.

---

[44] *See* Admin. Code § 23-1203(8).
[45] Available at https://www1.nyc.gov/site/moip/reports/reports.page.
[46] *See* Admin. Code §§ 23-1202(b)(2)(a) and (c)(2)(a).
[47] *See* Admin. Code §§ 23-1202(b)(1) and (c)(1).

4.3.3 Exemption for Collections and Disclosures Involving Police or Child Welfare 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 individual who is otherwise not legally competent.[48]

4.4 Reporting

4.4.1 Agency Reports

The Identifying Information Law requires agencies to submit a biennial report by July 31st in even-numbered years containing certain detailed information about their collection and disclosure of identifying information and their privacy practices.[49] The agency privacy officer should work with the agency head or their designee to support agency compliance with this obligation.[50] The agency may opt to submit additional information as the agency head believes is necessary for the report.

> ➢ **Guidance Tip**: The Mayor's Office of Information Privacy plans to update and streamline agency reporting templates for subsequent reporting years, such that information collected on the form is more useful for purposes of form completion and can be transmitted to a centralized, secure database. Additionally, the Office plans to use this centralized database during the next agency reporting process to archive the historical data that agencies have submitted to satisfy compliance, allowing agencies in future reporting periods to directly reference past reports and designations.

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[51] to the Chief Privacy Officer, as follows: June 16 through September 15th (1st Quarter); September 16 through December 15 (2nd Quarter); December 16th through March 15th (3rd Quarter); and March 16th through June 15th (4th Quarter). 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.[52] 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,[53] and makes such report available online.[54]

---

[48] *See* Admin. Code §§ 23-1202(b)(2)(c) and (c)(2)(c).
[49] *See* Admin. Code § 23-1205.
[50] The Agency Privacy Officer Toolkit is on file with the Mayor's Office of Information Privacy.
[51] The quarterly reporting dates track the effective date of the Identifying Information Law.
[52] This guidance is on file with the Mayor's Office of Information Privacy.
[53] *See* Admin. Code §§ 23-1202(c)(4) and (d)(2).
[54] *Id.* CPO quarterly reports are available at https://www1.nyc.gov/site/moip/reports/reports.page.

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 circumstances, even if the quarterly report is not yet due.[55] 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.[56] Agency privacy officers must document the collections and disclosures they have designated as routine and agencies must advise the appropriate agency staff and covered contractors and subcontractors of such pre-approvals.[57]

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.[58] 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 pre-approve the disclosure as "routine" and Agency B should pre-approve the collection of the same information from Agency A as "routine"). Agency privacy officers must communicate these approvals 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.

[55] *See* Admin Code § 23-1202(d)(1).
[56] *See* Admin. Code § 23-1201.
[57] The Agency Privacy Officer Toolkit is on file with the Mayor's Office of Information Privacy.
[58] *See* Admin. Code § 23-1201.

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 disclosures for agency functions as routine, agency personnel should strive to collect or disclose only the amount of identifying information 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.

"Routine" designations may cover fairly broad categories of agency functions, such as personnel administration, or responding to legal demands for information. Even where these types of collections and disclosures are categorically designated by the agency privacy officer as "routine" because they are part of the agency's normal course of business, the agency should still have internal protocols to ensure that the appropriate level of internal review and approval takes place for each collection or disclosure within that category. In other words, just because a function has been designated as routine for the agency does not mean that any and all identifying information can or should be collected or disclosed for that function without further internal agency review.

> ➢ **Guidance Tip:** For example, an agency privacy officer may categorically pre-approve disclosures of identifying information for "responding to subpoenas" as a "routine" function for the agency, but each subpoena contains specific demands for data to which various laws or privileges may apply. As such, the agency should have internal protocols in place that require review of the relevant laws, regulations, and any privileges governing the identifying information (and other information) named in each subpoena before the disclosure is made. As another example, where the function of "reporting to oversight agencies" has been designated as "routine," each request made by an oversight agency should be reviewed to make determinations such as whether any identifying information requested is governed by another law that would restrict its disclosure, or whether a confidentiality agreement is required.

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.[59] Such collections and disclosures are considered "non-routine."

> ➢ **Guidance Tip**: The agency privacy officer should consider making case-by-case ("non-routine") determinations where the collection or disclosure is a unique or non-recurring activity for the agency that does not take place during the normal course of the agency's business. Examples could include a disclosure for a one-time data-sharing project, or a new multi-agency study involving one or more other agencies.

When a request is received for a collection or disclosure of identifying information that has not been designated as "routine" and 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 inter-agency collections or disclosures of identifying information upon a determination that the collection or disclosure is in the best interests of the City.[60] Refer to **Section 5.2.3** on the Chief Privacy Officer's role in non-routine collections and disclosures.

> ➢ **Guidance Tip**: There may be overlap between the types of disclosures and collections that can be approved by the agency privacy officers and the Chief Privacy Officer. Agency privacy officers should contact the Chief Privacy Officer if they have any questions or concerns about making case-by-case determinations on requests for collections and disclosures of identifying information. Also see **Section 5.2.3** below for further information about the Chief Privacy Officer's authority in making such determinations.

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 following criteria, as well as other factors based on their agency's mission and purpose. If a majority of the considerations listed below weighs 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?
- 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?

[59] *See* Admin. Code § 23-1202(c)(3).
[60] *See* Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

- 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?

> ➢ **Guidance Tip**: To illustrate the distinction between making "routine" and "case-by-case" ("non-routine") designations, consider the following scenario: An agency wants to report demographic information about its employees to senior City officials in furtherance of an equity initiative related to City employment. Since demographic information is a type of identifying information, the agency must obtain approval from its agency privacy officer before disclosing it. Provided that no other law prohibits the disclosure, the agency privacy officer, at their discretion considering the facts concerning the proposed disclosure, may:
>
> (i) pre-approve it, in writing, as "routine" upon a determination that the disclosure furthers the purpose or mission of the agency and is a part of normal agency business – meaning, an activity that will likely recur, perhaps as part of the agency's EEO function. A "routine" designation will mean that agency privacy officer approval is not required for future disclosures of the identifying information for purposes of this function; or
>
> (ii) pre-approve it, in writing, on a "case-by-case" basis upon a determination that the disclosure furthers the purpose or mission of the agency since it is not a part of normal agency business – for example, where the equity initiative requires a single disclosure (or set of disclosures) of identifying information because this is a unique project, such as a new study relating to the City's workforce. A "case-by-case" designation will mean that the agency privacy officer's approval would be required for another project involving disclosures of this type of identifying information; or
>
> (iii) disapprove the disclosure upon a finding that it does not further the purpose or mission of the agency, and refer the matter to the Chief Privacy Officer, as appropriate.

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

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. When reviewing requests for identifying information from oversight agencies, the agency privacy officer should generally authorize the disclosure, subject to **Section 5.2.2.1** below, if:

(1) the oversight agency is legally entitled to request the information;

(2) the agency receiving the request is not restricted by law from disclosing the information to the oversight agency, and is not asserting a privilege relating to the requested information; **and**

(3) one of the following applies:

(i) the agency privacy officer has pre-approved the disclosure of the type of requested identifying information as "routine";[61] or

(ii) the agency privacy officer approves the disclosure, on a case-by-case basis, as being required by law; or

[61] *See* Admin. Code 23-1202(c)(2)(a).

(iii) the agency privacy officer approves the disclosure, on a case-by-case basis, as furthering the mission or purpose of the agency, subject to any confidentiality agreements and data security requirements necessary to protect the privacy and security of the information;[62] or

(iv) if the oversight agency is a City agency, where the Chief Privacy Officer pre-approves the collection and disclosure of the identifying information by, respectively, the oversight agency and disclosing agency, upon the determination that the collection and disclosure are in the best interests of the City.[63]

5.2.2.1 Requests Implicating Important Privacy Interests Including Sensitive Identifying Information

Where the disclosure of identifying information to the oversight agency is approved by the agency privacy officer (as "routine," or on a "case-by-case" basis), if the agency privacy officer or Chief Privacy Officer determines that disclosure of the requested information will involve a risk of compromising an important privacy interest—such as but not limited to where sensitive identifying information will be disclosed—a confidentiality agreement will be required, along with use of secure transmission and storage protocols that comply with the requirements of the Citywide Cybersecurity Program Policies & Standards for handling information classified as "Restricted" information.[64] If the disclosure of sensitive identifying information is required by law, agencies should also seek to obtain a confidentiality agreement before disclosing such information, and seek guidance from their agency privacy officer, other agency counsel, or the Chief Privacy Officer if they have difficulty obtaining such an agreement.

- **Guidance Tip**: The use of confidentiality agreements between City oversight agencies and other City agencies disclosing information to them is a practice that predates the enactment of the Identifying Information Law. Such agreements typically include commitments to safeguard information, report any unauthorized disclosures to the source agency, and inform the source agency of any subpoena or third-party request for the information to enable the source agency to take legal action in response. Model confidentiality agreements and assistance developing such agreements can be provided by the Chief Privacy Officer or Mayor's Office of Information Privacy.

- **Guidance Tip**: Examples of when a confidentiality agreement with an oversight agency would be appropriate include: where the requested identifying information could reveal: the identities or location of public benefit recipients, confidential informants, domestic violence survivors or other vulnerable individuals or populations; the City's fraud detection methodology or non-public information about the City's cybersecurity or infrastructure assets; or where the disclosure would reveal individuals' medical or mental health information, among others. Agency privacy officers may contact the Chief Privacy Officer for guidance in determining whether a confidentiality agreement with the oversight agency is required.

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

The Chief Privacy Officer may approve in advance (i) interagency 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.[65] 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

[62] *See* Admin. Code § 23-1202(c)(1)(b).
[63] *See* Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).
[64] *See* the Citywide Information Management Standard, available at http://cityshare.nycnet/html/cityshare/downloads/it_wireless/info_security_policies/Sensitive-CSP-Citywide-Information-Management-Standard.pdf.
[65] *See* Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

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 a "best interests of the City" determination.

> ➢ **Guidance Tip**: Prior to referring potential collections or disclosures of identifying information to the Chief Privacy Officer for a possible "best interests of the City" determination, agency privacy officers should consider whether a proposed collection or disclosure could be approved by the agency privacy officer, given the agency's subject matter expertise and legal authority under the Identifying Information Law to make such determinations about agency information.

5.3 Collections and Disclosures Involving Investigations

Neither agency privacy officer nor Chief Privacy Officer approval is required for collections and disclosures of identifying information: (i) 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 (ii) in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.[66]

5.4 Collections and Disclosures 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 is defined in this Policy to include emergency circumstances where the collection or disclosure of identifying information is so urgently necessary that the prior review and authorization by the agency privacy officer or the Chief Privacy Officer are not practicable, because it would create undue delays in responding to the emergency.[67]

> ➢ **Guidance Tip**: As examples, disclosing identifying information about known occupants of a building or area following a no-notice event, such as a gas explosion or emergency flooding condition, would be considered a disclosure under exigent circumstances because of the urgent need to address an imminent threat to the public health and safety. Under such conditions, it would be impracticable to implement normal agency privacy officer review procedures before disclosing identifying information—such as building occupants' names and contact information—because any delays in disclosure could impair evacuation and other emergency response efforts. Similarly, during a severe weather event where regularly scheduled City food delivery services to homebound individuals are not operational, disclosing individuals' contact information to an alternate City vendor to deliver emergency food for them would be considered exigent circumstances.

Information about the collection or request and disclosure made under exigent circumstances, along with an explanation of why exigent circumstances existed, must be reported to the agency privacy officer as soon as practicable after such 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).[68]

[66] *See* Admin. Code §§ 23-1202(b)(2)(c) and (c)(2)(c).
[67] Refer to **Section 3.2.4.**
[68] Refer to **Section 4.4.2** for details on reporting collections or disclosures made under exigent circumstances.

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.[69] 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.

> ➢ **Guidance Tip**: Agency privacy officers should consult with the Chief Privacy Officer and the Mayor's Office of Information Privacy on large-scale, multi-agency projects involving the collection and disclosure of identifying information so that appropriate privacy and data security protection language is included in such agreements.

5.5.1 Requests and Proposals for Sensitive Identifying Information

Requests or proposals for the collection or disclosure of sensitive identifying information require additional review by the agency privacy officer, or designated agency counsel, or 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 means minimizing the identifying elements of information contained in data sets, records, or other mediums. Agency privacy officers should coordinate with agency leadership to identify circumstances where it is appropriate, given the purpose and mission of the agency and relevant law, 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:

- *Aggregation*: Compiling data into a summary to de-identify it. For example, rather than sharing the names of each individual from a borough who submitted an application for a specific program, the agency could state how many people from a borough applied for the program.

- *Suppression*: Replacing data that refers to a small number of individuals with a designated value. For example, if there are three public benefits recipients residing at a given street address, replace "3" with "<5" (or a symbol, such as "*") to characterize the number of public benefit recipients living at the street address. Generally, agencies are advised to suppress any identifying number less than 5 to protect against risks of identifying or locating any person, unless the disclosure of identifying information is authorized by the agency privacy officer

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

(or Chief Privacy Officer), required by law, or exigent circumstances apply. Limiting disclosure of identifying information by using values of <5 through suppression, particularly where sensitive identifying information is involved, may be particularly useful in public reporting or evaluation.[70]

- *Pseudonymization*: Replacing identifying information with a non-identifying label or labels so the information cannot be attributed to an individual. For example, replacing a person's name with "A." Use caution when pseudonymizing data because simply re-labelling one type of information (data element) will not be effective if the record contains many other elements of identifying information that could still together re-identify the pseudonymized individual.

- *Redaction*: Removing identifying information before disclosing a record, such as by deleting birthdates from a document. When redacting, be sure to use methods that ensure the redacted text cannot be read (for physical copies, check both sides of the document).

- *Differential privacy*: Making available certain information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. When sharing sensitive statistical data, applying differential privacy techniques can help create a final dataset that does not reveal whether any one individual's identifying information was included in the original dataset.

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.

5.7 Retention of Identifying Information

Pursuant to Admin. Code § 23-1202(e), agencies must retain identifying information where required by law or City 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 their 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 records officers 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.

[70] Agencies may consider using a higher number, such as where sensitive identifying information is involved, and may find it beneficial to consult with a statistician for guidance in making such determinations.

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.[71] 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 Contracts Subject to the Identifying Information Law ("Covered Contracts")

Covered contracts must include the "Identifying Information Rider," which is attached to this Policy (**Appendix B**) and on file with the Mayor's Office of Information Privacy and the Law Department. 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.

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.[72] 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.[73]

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

The Chief Privacy Officer has designated two additional types of contracts for other services that will be subject to the requirements of the Identifying Information Law, **effective for any new contracts entered into or renewed on or after July 1, 2021**: (1) contracts and subcontracts for technology services involving sensitive identifying information collected by the contractor or subcontractor on behalf of the City;[74] and (2) certain contracts and subcontracts for outreach services involving identifying information, described respectively in **Sections 6.1.2.1** and **6.1.2.2** below.

---

[71] When disposing of records containing identifying information or certain electronic equipment, agencies should be aware of potential obligations under Admin. Code §§ 10-503 and 10-504, in addition to any other applicable laws, regulations, or policies.
[72] *See* Admin. Code § 23-1201.
[73] *See* Admin. Code §§ 23-1201 and 6-129(c)(21).
[74] "Sensitive identifying information" is defined in **Section 3.2.5** as "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."

The Chief Privacy Officer and Mayor's Office of Information Privacy will collaborate with the City's Law Department and relevant City agencies to create informational materials and protocols designed to support agencies whose contracts and contract renewals will be subject to the requirements of **Section 6.1.2**.

6.1.2.1 Contracts and Subcontracts for Technology Services Involving Sensitive Identifying Information

"Contracts and subcontracts for technology services involving sensitive identifying information" include contracts and subcontracts in which the contractor's or subcontractor's "technology" (as such term is defined by the State Technology Law[75]) or technology services are procured by the City and used by the contractor or subcontractor on behalf of the City to collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information,[76] or which make sensitive identifying information accessible to the contractor or subcontractor in connection with such contract or subcontract although such access may not be the express purpose of the contract.[77] This definition does not include: (i) contracts where the vendor simply provides a technology product to the City, such as basic computer hardware or on-premise software which does not involve the vendor's access to sensitive identifying information; or (ii) subcontracts for technology services that generally govern a contractor's business relationships as a whole (i.e., for a broad range of clients, and not just specifically the City), provided that the City contractor includes appropriately protective privacy and security provisions in such subcontracts.

"Contracts for "technology services involving sensitive identifying information" include City contracts through which the contractor or subcontractor receives, hosts, or otherwise has the capability to access sensitive identifying information, as determined by the agency that is the source of the identifying information, in consultation with its agency privacy officer, and the Chief Privacy Officer as necessary.

> ➢ **Guidance Tip**: Examples of such contracts include those: (i) where the contractor will use its technology to collect, from one or more City agencies, sensitive identifying information of City agency clients (or members of the public) to produce identification cards for them; and (ii) where the contractor hosts a cloud-based software application that enables City employees to upload sensitive identifying information to complete a confidential health questionnaire, the screening results are transmitted only to the employee's human resources department, but the contractor can technically access the employee's health information by virtue of hosting the platform.

6.1.2.2 Contracts and Subcontracts for Outreach Services Involving Identifying Information

"Contracts and subcontracts for outreach services involving identifying information" include contracts and subcontracts where the contractor or subcontractor collects, uses, or discloses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events, through any means. The agency that is the source of the identifying information, in consultation with its agency privacy officer and the Chief Privacy Officer as necessary, shall identify such contracts and subcontracts. "Accessing information about City services, resources, or events" includes learning about, obtaining, enrolling in, participating in, registering for, or otherwise receiving City services. Methods of access include, are but not limited to, in-person or telephone contact, text-messaging, email, mail, or website postings. For clarification, this designation of certain outreach contracts only applies to projects led by one City agency or office which engages a vendor to perform outreach on behalf of other City agencies for the benefit of their

[75] *See* N.Y. State Technology Law § 101(5) ("'Technology' means a good, service, or good and service that results in a digital, electronic or similar technical method of achieving a practical purpose or in improvements in productivity, including but not limited to information management, equipment, software, operating systems, interface systems, interconnected systems, telecommunications, data management, networks, and network management, consulting, supplies, facilities, maintenance and training").
[76] Refer to **Section 3.2.5** for guidance on sensitive identifying information, including security standards for such information.
[77] This may include but is not limited to identifying information belonging to individuals applying for or receiving City services.

clients. This designation does not include agency contracts with a vendor to perform outreach services to the agency's own clients; however, agencies using vendors to conduct outreach to their own clients through contracts and subcontracts that are not covered contracts under this Policy are encouraged to attach the Privacy Protection Rider (**Appendix F**) to these contracts.

> ➢ **Guidance Tip**: Examples of a "Contract for Outreach Services involving Identifying Information" would include a citywide initiative conducted by a lead agency or office to enroll New Yorkers in health insurance or Pre-K programs, encourage participation in the Census, or to provide information about emergency services to the clients of one or more City agencies or offices (or members of the public), where a contractor or subcontractor will collect the identifying information of one or more City agency's or office's clients (or members of the public), other than the lead agency or office, for purposes such as emailing, texting, or mailing them information about available City services, or to notify them of an upcoming town hall, or to provide information about a public benefit program for which they may be eligible.

6.1.3 Non-Covered Contracts Involving the Collection, Use, and Disclosure of Sensitive Identifying Information

When a contract or subcontract of any value involves the collection, use, or disclosure of sensitive identifying information, but is not a "covered contract" as defined in this Policy, it is strongly recommended that agencies include provisions in those contracts to appropriately protect the privacy and security of such information, by attaching the Privacy Protection Rider (**Appendix F**) to such contracts.

If the contract or subcontract involves sensitive identifying information and is not a "covered contract" as defined in this Policy, and an agency does not attach the Privacy Protection Rider to it, guidance for drafting provisions to protect the privacy and security of such information is available in **Appendix H.**

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 between the City agency and a third party,[78] the disclosing City agency must enter into a data sharing agreement with such third party in certain circumstances.[79] 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. Refer to **Appendix H** for guidance on drafting contracts involving collections or disclosures of sensitive identifying information;
- Disclosures of identifying information that are restricted by other laws or regulations;

[78] The term "third party" here includes, but is not limited to, other City agencies.
[79] *See* Admin. Code § 23-1203(4).

- 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 format 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 protection protocols for interagency 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.[80]

> ➢ **Guidance Tip**: Refer to **Section 5.2.2** for responding to requests for identifying information from oversight agencies, and drafting agreements when such requests involve disclosure of sensitive identifying information.
>
> ➢ **Guidance Tip**: Refer to **Appendix H** for guidance on drafting agreements or contracts that involve disclosure of sensitive identifying information.

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 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.

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

7.0 Training and Education Requirements

7.1 Citywide Privacy Training

The Chief Privacy Officer, through the Mayor's Office of Information Privacy, has worked with relevant agencies, including representatives of the Citywide Privacy Protection Committee, the Department of Citywide Administrative Services, DoITT/Cyber Command, Law Department, and other relevant City agencies to develop and implement citywide privacy protection training, adaptable by agencies, for use with their employees and covered contractors and subcontractors on the requirements imposed by the Identifying Information Law and this Policy, along with a strategy for tracking completion of the training by appropriate personnel. The Chief Privacy Officer, in consultation with such agencies and through other research, continues to 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 materials, and will address other matters including frequency of training, mechanisms for updates, and issues relating to implementation of mandatory training for new hires.

- **Guidance Tip**: The Chief Privacy Officer, through the Mayor's Office of Information Privacy and in partnership with the Department of Citywide Administrative Services' Learning and Development Unit, created baseline citywide privacy training for all City employees (Module A). A pilot project involving various agencies and different job titles has been implemented and plans are underway for an expected citywide rollout of Module A in 2021. Module B, a more advanced training suited for personnel whose primary job function involves handling of identifying information (e.g., attorneys, open data coordinators, and HR professionals), is currently in development.

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, 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.

> ➢ **Guidance Tip**: As part of the 2020 biennial compliance cycle, the Chief Privacy Officer, through the Mayor's Office of Information Privacy, executed an outreach strategy to educate community boards on their reporting requirements for compliance with the Identifying Information Law, which included webinars and virtual office hours, coordination with the General Counsel at each Borough President's Office, and collaboration with the Mayor's Community Affairs Unit. Further efforts will be made to address the unique staffing and other needs of community boards with respect to compliance, including provision of additional training, model workflows and templates for reporting, in addition to other guidance specific to issues and concerns unique to community boards.

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).

> ➢ **Guidance Tip**: The Chief Privacy Officer reviews each agency report of a violation of the Identifying Information Law. As appropriate, the Chief Privacy Officer contacts the reporting agency privacy officer to learn more about the facts underlying the report to determine whether further action is necessary, such as, but not limited to, additional fact gathering and any notification requirements, and to collaborate on measures to reduce or prevent similar violations in the future.

8.2 Receiving and Investigating Complaints

City agencies must adopt written protocols for receiving and investigating complaints[81] under the Identifying Information Law which, at a minimum:

- 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;[82] 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. Additionally, each agency privacy officer is strongly encouraged to publish their agency's written protocols on the agency's website.

Agency privacy officers should immediately notify the Chief Privacy Officer if they know or suspect that an individual's identifying information has been improperly accessed, used, disclosed, or otherwise revealed. The Chief Privacy Officer will notify other relevant City officials, such as, but not limited to the Law Department and Cyber Command, as necessary, to coordinate and advise on any further investigation and response.

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 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 the City's Law Department, that notification[83] to such individuals should occur.

[81] 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.
[82] *See* Admin. Code § 23-1202(c)(4).
[83] In addition to notification, other actions may be appropriate under the circumstances. For example, credit monitoring may be advisable where Social Security number or bank account information has been disclosed in violation of the Identifying Information Law. If home address has been improperly released, such as for a domestic violence survivor, recommending a change of door locks

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.

may be warranted. Each complaint must be reviewed by the agency and relevant City officials on a fact-specific basis to determine applicable laws and requirements, appropriate mitigation steps, and any other actions.

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
- NYC Water Board
- 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

Page Intentionally Blank

Mayor's Office of Information Privacy

Appendix B – Identifying Information 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 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. "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 Chief Privacy Officer, and any other category of information designated by the 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 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 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 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 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.

Section 1.07 Reporting.

Contractor shall provide the Agency with reports as requested by the Agency Privacy Officer or 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 Chief Privacy Officer; and (c) any other related information that may be reasonably required by the Agency Privacy Officer or 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 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 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 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. 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

#	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.	• 3.2.1 Anonymization • 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.	• 1.5.2 Agency Privacy Policies, Protocols, and Practices • 4.2.1 Agency Privacy Protection Policies and Guidance • 4.2.2 Agency Compliance Plan
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.	• 5.2.2.1 Requests Implicating Important Privacy Interests Including Sensitive Identifying Information • 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" • 5.2.3 Chief Privacy Officer Role in Non-Routine Collections and Disclosures
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.	• 1.6.3 Local Law 45 of 2005 and Local Law 11 of 2017 • 8.3 Notification Requirements • Appendix B (Identifying Information Rider) • Appendix F (Privacy Protection Rider) • Appendix H (Guidance for Drafting Contract Terms to Protect Sensitive Identifying Information)
7	Establish standard contract provisions, or required elements of such provisions, related to the protection of identifying information.	• 6.1.1 Contracts and Subcontractors Subject to the Identifying Information Law • 6.1.2.2 Contracts and Subcontracts for Outreach Services Involving Identifying Information • 6.1.3 Non-Covered Contracts involving the Collection, Use, and Disclosure of Sensitive Identifying Information • 6.2.2 Elements of Data Sharing Agreements • Appendix B (Identifying Information Rider) • Appendix F (Privacy Protection Rider) • Appendix G (Guidance for Relevant Privacy Attachments)
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 • 4.2.2 Agency Compliance Plan
9	Establish a mechanism for accepting and investigating complaints for violations of this chapter.	• 8.2 Receiving and Investigating Complaints

Mayor's Office of Information Privacy

Appendix E – Sample Mutual Non-Disclosure Agreement for External Parties

This Non-Disclosure Agreement (**NDA**) is between the City of New York, acting through [agency], located at [agency address], and [Vendor], including its current and future affiliates, a [describe Vendor's business], with its primary offices at [Vendor's address] (each a **Party** and collectively the **Parties**), in relation to [describe project] (**Project**).

1. The City and [Vendor] agree to collaborate on the Project for the purpose of [Permitted Purpose]. In furtherance of this goal, [Vendor] will [describe Vendor's role]. The Parties may have access to each other's Confidential Information, as such term is defined below, subject to the terms of this NDA.

2. **Definitions**.

    a. **Authorized Users** means employees, officials, and agents of the Receiving Party whose access to Confidential Information is necessary to carry out the Permitted Purpose.

    b. **Confidential Information** means non-public information that the Disclosing Party discloses to the Receiving Party under this NDA, in any form; information derived from non-public information or from information marked as private or confidential; Identifying Information, other than routine business contact information; any other information that a reasonable person knows or should understand to be confidential; and any information that could, if disclosed, reveal the Disclosing Party's proprietary or trade secret information. Confidential Information **does not include** information that is publicly available or known to the Receiving Party prior to its disclosure by the Disclosing Party; is independently developed by the Receiving Party without reference or access to Confidential Information; or is lawfully obtained by the Receiving Party without restrictions on use or disclosure from a third party.

    c. **Disclosing Party** means the Party disclosing its Confidential Information.

    d. **Permitted Purpose** means a use of a Party's information that is necessary to carry out the Party's duties in relation to the Project.

    e. **Identifying Information** means information that alone or in combination with other information could be used to identify or locate a person.

    f. **Receiving Party** means the Party receiving Confidential Information.

3. **Scope.** The restrictions on collection and disclosure of Identifying Information apply to information that [Vendor] has received from the City or has otherwise acquired for purposes of this NDA.

4. **Confidential Information.**

    a. Except in connection with a Permitted Purpose, the Receiving Party will not disclose Confidential Information without the Disclosing Party's written permission, subject to 4(e) below. If [vendor] is the Receiving Party, it will not use Confidential Information in any of its business operations except as needed to process requests or evaluate proposals by [agency], and will not use Confidential Information for any purpose except as authorized under this NDA or as required by law. The Receiving Party will limit access to Confidential Information to Authorized Users for the Permitted Purpose, and will ensure that Authorized Users understand and comply with the provisions of this agreement applicable to Confidential Information.

b. Except as authorized under this NDA, or an agreement incorporating this NDA by reference or to which the NDA is attached, the Receiving Party will not use Confidential Information for personal benefit or the benefit of another, nor publish, sell, license, distribute, or otherwise reveal Confidential Information.

c. The Receiving Party will use appropriate physical, technological, and procedural safeguards to protect Confidential Information. If the Receiving Party is [agency], these safeguards will conform to the citywide security standards and data security requirements set forth by the New York City Department for Information Technology and Telecommunications and the NYC Cyber Command. If the Receiving Party is [agency], it will treat Confidential Information as ["restricted" or "sensitive"] information under the Citywide Cybersecurity Program Policies and Standards. If the Receiving Party is [vendor], it will treat Confidential Information as required by the Cybersecurity Requirements for Vendors & Contractors, available at https://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page.

d. If the Receiving Party knows or suspects unauthorized use or disclosure of Confidential Information, it will promptly

    i. notify the Disclosing Party, no later than seventy-two hours after discovery, of:

        1. the discovery of the known or suspected unauthorized use or disclosure;
        2. the date of the use or disclosure;
        3. the name of the user or recipient, if known;
        4. the address of the user or recipient, if known;
        5. the affiliation of the user or recipient, if known;
        6. a brief description of the information used or disclosed;
        7. a description of any remedial measures taken to mitigate the effects of such unauthorized use or disclosure of Confidential Information, in accordance with all relevant laws;
        8. any details necessary for the Disclosing Party to know when and how the unauthorized use or disclosure was made;

    ii. cooperate with the Disclosing Party and relevant City officials, including the City's Chief Privacy Officer, NYC Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the unauthorized use or disclosure, and make any required or voluntary notices; and

    iii. take all reasonably necessary steps to prevent or mitigate damages related to the unauthorized use or disclosure.

e. The Receiving Party may disclose Confidential Information if required by court order or law. If the Receiving Party is required to disclose Confidential Information by law, it will:

    i. promptly notify the Disclosing Party sufficiently in advance of disclosure, but not more than five business days after it learns of the required disclosure, to permit Disclosing Party to seek a protective order and to make any required notifications; and

    ii. disclose Confidential Information only to the extent allowed under a protective order or as necessary to comply with the law.

f. If the Disclosing Party instructs the Receiving Party to destroy Confidential Information, the Receiving Party will destroy it no more than five business days after receiving the instruction. The Receiving Party will inform the Disclosing Party that it has destroyed the Confidential Information no more than thirty days after receiving the Disclosing Party's instruction. If it is impossible for the Receiving Party to destroy Confidential Information, the Receiving Party will explain in writing why it is impossible, and

will, upon receiving the Disclosing Party's destruction request, immediately stop accessing or using the Confidential Information.

5. **General rights and obligations.**

   a. **Law that applies; jurisdiction and venue**. The laws of the State of New York govern this NDA. If federal jurisdiction exists, the federal courts in New York County, New York, have exclusive jurisdiction and venue. If federal jurisdiction does not exist, the Supreme Court in New York County, New York, has exclusive jurisdiction and venue.

   b. **Waiver.** If [agency] is the Disclosing Party, its delay or failure to exercise a right or remedy is not a waiver of that, or any other, right or remedy.

   c. **Money damages insufficient.** Money damages may be an insufficient remedy for breach or threatened breach of this NDA by the Receiving Party. In addition to all other remedies that the Disclosing Party may have, the Disclosing Party will be entitled to specific performance and injunctive or other equitable relief as a remedy for any breach of the confidentiality and other obligations of this NDA.

   d. **Enforceability; severability.** If any part of this NDA is unenforceable, the Parties (or if they cannot agree, a court) will revise it so that it is enforceable. Even if no revision can be enforced, the rest of the NDA will remain in place.

   e. **Intellectual property.** This NDA does not give the Receiving Party any intellectual property ownership of or licenses to Confidential Information.

   f. **Entire agreement.** This NDA is the entire agreement between the Parties about disclosing Confidential Information in relation to the its subject matter, except that if other contracts between the Parties address Confidential Information, then those obligations remain in force for those contracts.

   g. **Modifications.** The Parties can only modify this NDA in writing.

   h. **Notices.** Notices must be in writing and may be sent by email. Notices must be sent to the following people or their designees:

      i. **For the City:**

      ii. **For Vendor:**

Mayor's Office of Information Privacy

Appendix F – Privacy Protection Rider

Privacy Protection Rider

(To supplement contracts of any value with the City of New York that are not "covered contracts"[84] under the Identifying Information Law, but which the City's Chief Privacy Officer has determined are the types of contracts for services that require additional privacy protection provisions because: (1) the contract involves the collection, use, or disclosure of, or access to "Sensitive Identifying Information"[85] of members of the public or City employees or officials; or (2) the nature of the Identifying Information and the circumstances of its collection or potential disclosure by Contractor implicate an important privacy risk.)

Purpose.

The Chief Privacy Officer has determined that, in connection with the type of services provided under this Agreement, Contractor may collect, use, disclose, access, and retain Sensitive Identifying Information only in accordance with the requirements of this Privacy Protection Rider ("Rider"), other provisions of this Agreement, and as otherwise required by law.

A. Definitions.

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

ii. "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.

iii. "Authorized User," as it relates to collection, use, disclosure of, or access to Identifying Information under this Agreement, means a Contractor whose collection, use, disclosure of, or access to Identifying Information is necessary to carry out the activities and obligations set forth in this Agreement, or is required by law.

iv. "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.

[84] Laws 245 and 247 of 2017 (codified at New York City Charter ("Charter") Section 8 subdivision (h) and Sections 23-1201 to -1205 of the Administrative Code of the City of New York ("Admin. Code"), collectively, the "Identifying Information Law") went into effect on June 15, 2018. Such laws apply to "human services" contracts and subcontracts and other contracts designated by the Chief Privacy Officer that involve the collection, retention, or disclosure of "Identifying Information" in connection with services provided under a City contract or subcontract ("covered contracts"). The Identifying Information Rider (and not the Privacy Protection Rider) applies to covered contracts.

[85] "Sensitive Identifying Information" means 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.

v. "Contractor" for purposes of this Rider, means the entity entering into a contract with the City and includes employees, subcontractors, and agents of Contractor unless the context requires otherwise.

vi. "Exigent Circumstances" means 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.

vii. "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, 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 Chief Privacy Officer, and any other category of information designated by the Chief Privacy Officer, including but not limited to: an individual's Social Security number, date of birth, Internet Protocol ("IP") address; taxpayer identification number; device identifier, 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; social media account information; and any identifier that can identify an electronic device linkable to an individual.

viii. "Permitted Use" means the use of Identifying Information only as necessary to carry out the activities described in this Agreement.

ix. "Sensitive Identifying Information" means Identifying Information which a City agency privacy officer or the City's Chief Privacy Officer has determined that alone, or in combination with other information may, based upon its very nature or under specific facts and circumstances, poses 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.

x. "Source Data" means Identifying Information that was initially collected by an agency that maintains such information within such agency's recordkeeping system.

B. Scope.

The restrictions on collection, use, disclosure of, and access to Identifying Information apply to information that Contractor has received from the City or has otherwise acquired for purposes of this Agreement.

C. Collection.

Absent Exigent Circumstances, Contractor shall not collect Identifying Information unless such collection (a) has been pre-approved in writing by the Agency collecting it, in consultation with its Agency Privacy Officer or other agency counsel, the Chief Privacy Officer, and other Agency staff as necessary, 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 by the New York City Police Department in connection with a criminal investigation; or (d) is by a City agency in connection with the welfare of a minor or other individual who is not legally competent. If the Identifying Information to be collected by Contractor, with an Agency's approval, is Source Data from one or more other Agencies, the agency privacy officers from the respective agencies shall coordinate with each other to determine whether the collection is appropriate. The Agency Privacy Officer of the Agency approving Contractor's collection of the Identifying Information will determine whether the collection is authorized.

D. Disclosure.

i. 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 pre-approved in writing by the Agency, in consultation with the Agency Privacy Officer, other agency counsel, the Chief Privacy Officer, and other Agency staff as necessary, 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 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, subject to Section E(iii). If the Identifying Information to be disclosed by Contractor, with an Agency's approval, is Source Data from one or more other Agencies, the agency privacy officer from the contracting Agency shall coordinate with the source Agency or Agencies to determine whether the disclosure is authorized.

ii. Contractor shall not make use of Identifying Information for the benefit of another, nor shall Contractor publish, sell, license, distribute, or otherwise reveal the Identifying Information without the prior written authorization of the individual or by such other person with legal authority to consent on behalf of the individual, or prior written approval of the Agency Privacy Officer or other agency counsel. Except as authorized in this Agreement, all third-party requests for Identifying Information received by the Contractor shall be promptly communicated to the Agency upon receipt and handled by the Contractor following the directions of the Agency Privacy Officer or other agency counsel, unless otherwise required by law.

iii. If disclosure of the Identifying Information by Contractor is required under the provision of any subpoena, judicial or administrative order, or otherwise pursuant to applicable law, Contractor shall: (a) as soon as practicable, but in no event later than five (5) business days from receipt of said subpoena, judicial or administrative order, or request pursuant to applicable law requiring such disclosure, notify the Agency Privacy Officer or other agency counsel in order to allow the 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, judicial or administrative order, or applicable law.

E. 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 the Agency Privacy Officer or other agency counsel 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 but not to exceed seventy-two (72) hours. 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. If the Agency determines the collection or disclosure was not made under Exigent Circumstances, the collection or disclosure shall be considered an unauthorized collection or disclosure pursuant to Section F below.

F. Unauthorized Collection, Use, or Disclosure of, or Access to Identifying Information.

i. If an individual's Identifying Information is collected, used, disclosed, or accessed, without authorization in violation of this Rider, Contractor shall promptly notify the Agency Privacy Officer (providing the information required in Section G(iv) below), in no event more than seventy-two (72) hours from the discovery of such unauthorized collection, use, disclosure, or access so that the Agency can investigate the incident.

ii. If such collection, use, disclosure, or access requires notification to the affected individual(s) pursuant to any law or the policies and protocols promulgated by the Chief Privacy Officer under subdivision 6 of Section 23-1203, at the direction of the Agency Privacy Officer, Contractor shall (a) make reasonable efforts to notify such individual(s) in writing of the Identifying Information disclosed or accessed and to whom it was disclosed or accessed as soon as practicable, or (b) cooperate with the Agency's efforts to notify such individual(s) in writing.

iii. Contractor shall take all reasonably necessary steps to prevent or mitigate the effects of the unauthorized collection, use, disclosure, or access.

iv. Contractor's notice to the Agency shall include a description of the nature of the incident resulting in an unauthorized collection, use, or disclosure of, or access to the Identifying Information, the type(s) of Identifying Information that may have been used, disclosed or accessed, 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 collection, use, disclosure, or access, in accordance with all relevant laws and regulations.

v. Contractor shall fully cooperate with the City's investigation of the incident resulting in an unauthorized collection, use, or disclosure of, or access to the Identifying Information. Cooperation, as requested by the City and/or its designees, shall include but not be limited to:

a. Providing information relating to Contractor's security controls, processes, and the relevant incident. This includes making available to the City and/or its designees all relevant reports and records, certifications, documented policies and procedures, self-assessments, independent evaluations and audits, view-only samples of security controls, logs, files, data reporting, incident reports or evaluations, remedial measures, verbal interviews with Contractor employees, subcontractors, and other individuals with knowledge of Contractor's security controls, processes and/or the relevant incident, and other materials required for either or both the City and Contractor to comply with applicable law or as otherwise requested by the City and/or its designees;

b. Providing the name, e-mail address, phone number, and title of a contact with sufficient knowledge and authority who shall respond promptly to City representatives in the event of unauthorized collection, use, or disclosure of, or access to Identifying Information. Contractor shall notify the Agency Privacy Officer in writing if this contact changes;

c. Submitting to an evaluation or audit by the City and/or its designees of Contractor's security controls, processes, and the relevant incident;

d. Conducting an evaluation or audit of Contractor's security controls, processes, and the relevant incident and providing the results of such evaluation or audit to the City and/or its designees; and

e. Obtaining an independent evaluation or audit of Contractor's security controls, processes, and the relevant incident and providing the results of such independent evaluation or audit to the City and/or its designees.

vi. 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 Chief Privacy Officer to address the unauthorized disclosure, 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 an unauthorized 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.

vii. Section G(i) shall not require any notification that would violate any law or interfere with an investigation or otherwise compromise public safety pursuant to subdivision c of Section 23-1205.

G. Additional Requirements.

i. In connection with this Agreement, collection, use, or disclosure of, or access to Identifying Information is restricted to "Authorized Users" for a "Permitted Use."

ii. Contractor shall ensure that effective physical, technological, and procedural safeguards are in place to protect the security of Identifying Information, including but not limited to ensuring that its personnel, subcontractors, and agents understand their obligations under this Agreement and applicable laws and regulations. Contractor 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 Contractor's custody.

iii. Contractor shall comply with the Citywide Cybersecurity Requirements for Vendors and Contractors set forth by the New York City Department of Information Technology and Telecommunications (DoITT) and New York City Cyber Command (NYC3), as they relate to Identifying Information, which are available at https://nyc.gov/infosec. Contractors shall comply with such Requirements as they may be modified from time to time.

H. 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, other agency counsel, or the Chief Privacy Officer.

I. Destruction.

If the Agency instructs Contractor to destroy Identifying Information obtained in connection with this Agreement, Contractor shall destroy it within five (5) business days after receiving the instruction, subject to any litigation holds. Contractor shall provide written confirmation to the Agency Privacy Officer that it has destroyed the Identifying Information within thirty (30) days after receiving the instruction. If it is impossible for Contractor to destroy the Identifying Information, Contractor shall promptly explain in writing why it is impossible, and shall, upon receiving the destruction request, immediately stop accessing or using the Identifying Information, and shall maintain such Identifying Information in accordance with this Rider.

J. Reporting and Coordination.

Contractor shall provide the Agency with reports, as requested by the Agency Privacy Officer, other agency counsel, or Chief Privacy Officer, regarding the collection, use, retention, disclosure of, and access to Identifying Information by Contractor, and including any other related information that may be reasonably required by the Agency Privacy Officer or Chief Privacy Officer. Contractor shall comply with directions of the Agency Privacy Officer, other agency counsel, and Chief Privacy Officer concerning reporting and coordination in relation to this Agreement.

K. 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, Article 5 of Appendix A (General Provisions Governing Contracts for Consultants, Professional, Technical, Human, and Client Services); or if Article 5 of Appendix A does not apply, the Investigations Clause.

L. Subcontracts.

i. Contractor shall include this Rider in all subcontracts to provide services in connection with this Agreement.

ii. Contractor agrees that it is fully responsible to the Agency for the compliance with this Rider by its subcontractors in connection with this Agreement.

M. Disclosures of Identifying Information to Third Parties.

Contractor shall comply with the Citywide Privacy Protection Protocols of the Chief Privacy Officer concerning requirements for a written agreement governing the disclosure of Identifying Information to a third party.

N. Construction.

As between the provisions of this Rider and the provisions elsewhere in this Agreement (including any attachment thereto), the more restrictive provision will control. The provisions of this Rider do not replace or supersede any other obligations or requirements of this Agreement.

Mayor's Office of Information Privacy

Appendix G – Guidance for Relevant Privacy Attachments

Note: Some agreements may require multiple attachments.

Type of City Contract	Attachment
Is this a contract for any consultant, professional, technical, human, and/or client services, valued at $100,000 or above?	Law Department Appendix A must be attached, except for certain types of contracts, including: purchases from State or federal contracts; contracts with a governmental entity; preferred source contracts; or contracts where the Law Department uses Rider 1 instead. (For further information on these and other exceptions, contact the Law Department.)
Is this a human services contract of any value?	Identifying Information Rider must be attached.
Is this a contract of any value for services that the Chief Privacy Officer has formally designated as being subject to the requirements of the Identifying Information Law (i.e., technology services involving sensitive identifying information or certain outreach services involving identifying information) ("covered contracts")?[86]	Identifying Information Rider must be attached.
Does this contract require additional privacy protections because: (1) the contract involves the collection, use, disclosure of, or access to sensitive identifying information of members of the public or City employees or officials; or (2) the nature of the identifying information and the circumstances of its collection or potential disclosure by Contractor implicates an important privacy risk?	Privacy Protection Rider should be attached.
Does this contract include the collection, use, disclosure of, or access to identifying information that is protected by a New York State or federal law? (Or, if applicable to the transaction, another state's laws?)	Incorporate appropriate privacy and data security provisions into the contract. Adjust these provisions as needed to ensure compliance with relevant federal or state laws and regulations.
Does this contract involve the purchase, lease, or licensing of cloud-based technology services such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), or Platform-as-a-Service (PaaS), or any other cloud services where access to City data is involved, regardless of whether identifying information is present?	DoITT's Cloud Services Agreement or provisions contained therein may be included.
Is the contract for the purchase of professional services involving access to City technology or City data?	DoITT's Attachment SCY must be attached.

[86] Refer to **Section 6.1.2** for definitions and additional guidance about these designated services.

Mayor's Office of Information Privacy

Appendix H – Guidance for Drafting Contract Terms to Protect Sensitive Identifying Information

The questions and sample provisions below are provided to help agencies draft contract provisions to protect sensitive identifying information for contracts that are not "covered contracts" as such term is defined in this Policy.

1. Granting Non-City Entities Permission to View, Collect, or Disclose Sensitive Identifying Information

Question: Will the contractor or subcontractor view, collect, or disclose any sensitive identifying information?

Guidance: If so, include provisions that specifically identify the information, at the data element level, to be treated as "sensitive" (and include the definition of "Sensitive Identifying Information" provided in this Policy). Agencies should also specify which individual users (or groups of users) will be permitted to access the sensitive identifying information, and the specific purpose for which access is permitted. The provisions should specify the degree of care[87] and the measures that those with access should use when handling or accessing the Sensitive Identifying Information.

In addition, if the agreement does not include DoITT Attachment SCY, it should include protocols that explain how to handle suspected or known data security incidents, such as a data security "breach," or an unauthorized disclosure of Sensitive Identifying information or other confidential information, and requirements for cooperating with City agencies in investigating and handling such incidents. These provisions should also include required timeframes for notifying other parties, including: notifying affected individuals where required by law; requiring mitigation efforts to prevent or minimize any harm that could result from such incidents; and safeguards against re-disclosure.

Sample language: Contractor shall hold all Confidential Information, including Sensitive Identifying Information, in strict confidence. Contractor shall only use Confidential Information in the good-faith performance of its obligations under this Agreement. Contractor shall immediately notify Agency in writing upon discovery of any actual or suspected improper use or disclosure of Confidential Information (**Improper Use or Disclosure**), which shall include, without limitation, any improper collection, access, use, disclosure, or release of Confidential Information other than as authorized by this Agreement or applicable law. In the event that Contractor discovers or suspects any improper use or disclosure of any Confidential Information, Contractor shall promptly, but no later than 72 hours of such incident, notify Agency of same, and shall take all reasonable steps to mitigate the impact of such Improper Use or Disclosure, and cooperate with Agency to investigate and prevent any further improper use or disclosure of Confidential Information. Improper Use or Disclosure of Confidential Information constitutes a breach of this Agreement and may lead to termination of this Agreement, among other remedies available in law or equity to Agency.

2. Prohibiting Third Parties from Viewing, Collecting, or Disclosing Sensitive Identifying Information

Question: Does the agency want to prohibit the contractor from allowing third parties to view, collect, disclose, or otherwise access some or all Sensitive Identifying Information that is available to the contractor or its subcontractor through the City contract?

[87] Typical standards of care require a contractor or subcontractor to exercise at least the same degree of care that the contractor or subcontractor uses to preserve the confidentiality of its own information of similar character, but in any event, at least a reasonable degree of care.

Guidance: The agreement should specify the type of Sensitive Identifying Information that the contractor must not disclose to third parties, as well as the circumstances when the contractor is authorized to disclose such information to any specific third parties.

Sample language: Notwithstanding the restrictions to disclosure set forth above, Contractor may disclose Sensitive Identifying Information as required by judicial order, lawfully issued subpoena, other order or notice of a court or administrative body of competent jurisdiction, or as otherwise required by law. If Contractor receives such a request, Contractor must provide written notice to Agency within five (5) business days of receiving the request, before disclosing Sensitive Identifying Information in response to the request, in order to permit Agency to seek an appropriate protective order or other legal relief. Contractor shall not otherwise disclose Sensitive Identifying Information to any third parties without the Agency's prior written authorization.

3. Authorizing Contractors or Subcontractors to Retain Sensitive Identifying Information

Question: Will the contractor or its subcontractors seek or need to retain any Sensitive Identifying Information?

Guidance: If so, the agreement should specify the length of time that the contractor may retain the Sensitive Identifying Information, and require that the contractor confidentially maintain such information unless disclosure is authorized by the contract or required by law. The agreement should state that the provisions relating to confidentiality will survive termination of the agreement. The agreement should also include terms that explain requirements for data destruction or return to the City, including any certification of destruction by contractor, or where such requirements are infeasible for providing written justification.

Sample language: Upon the termination of this agreement for any reason, Contractor shall return to Agency, or destroy (unless otherwise required by law), all Sensitive Identifying Information in any form that Agency disclosed to Contractor in connection with this Agreement, including copies and abstracts thereof, within thirty (30) days of termination. Contractor must confirm such data destruction in writing within sixty (60) days of this Agreement's termination, and provide a certificate of destruction where requested by Agency. If Contractor determines that returning or destroying any or all of the Sensitive Identifying Information is infeasible, Contractor shall promptly provide to Agency written justification and an explanation of the conditions that make return or destruction infeasible. In such instance, Contractor shall extend the protections of this Agreement to all Sensitive Identifying Information for which return or destruction is infeasible, and shall limit further uses and disclosures of Sensitive Identifying Information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains Sensitive Identifying Information.

4. Authorizing Contractors to Conduct Data Analysis involving Sensitive Identifying Information to Improve Agency Services, or Using De-Identified, Anonymized, Pseudonymized, or Aggregated Data Derived from Sensitive Identifying Information

Question: Has the contractor requested, and does the Agency wish to authorize, contractor's use of any sensitive identifying information provided or made available by the City through a contract, including any de-identified, anonymized, pseudonymized (assignment of random or artificial identifiers), or aggregated data derived from such sensitive identifying information, to conduct its own data analyses beyond the contracted purpose?

Guidance: If so, the agreement must expressly detail the specific type of Sensitive Identifying Information that the contractor proposes to analyze, including each data element, the purpose for which such information will be used, and the individuals or groups of individuals who will be authorized to access such information, and how the Sensitive Identifying Information will be used for data analysis. The agreement should also explain how the data will be returned or destroyed (see example 3 above).

Sample language: Notwithstanding any contrary terms, for Contractor's own use, Contractor shall be authorized to collect and analyze data and other information relating to the provision, use, and performance of various aspects of the [Services,

defined term] and related systems and technologies in accordance with its privacy policy, except for Sensitive Identifying Information. Contractor may, however, during and after the term of this agreement, use Sensitive Identifying Information and other data in a de-identified, anonymized, pseudonymized, or aggregated form to improve and enhance the Services and for other development, diagnostic, and corrective purposes in connection with the Services and other Contractor offerings.

5. Restricting or Prohibiting Use of De-identified, Anonymized, Pseudonymized, or Aggregated Sensitive Identifying Information by Contractors

Question: Does the agency want to restrict or prohibit a contractor from using Sensitive Identifying Information in a de-identified, anonymized, pseudonymized, or aggregated form to conduct its own data analysis?

Guidance: If the agency wants to restrict or prohibit a contractor from using de-identified, anonymized, pseudonymized, or aggregated data that includes Sensitive Identifying Information other than for uses authorized in the agreement, the agreement should clearly and explicitly state such restrictions.

Sample language: Contractor shall not use or retain Sensitive Identifying Information for any use other than uses authorized in this Agreement, without Agency's prior written approval. This restriction applies to Sensitive Identifying Information in any form, including information that has been de-identified, anonymized, pseudonymized, or aggregated.

6. Public Statements or Press Releases Concerning Sensitive Identifying Information

Question: Does the agency anticipate that the contractor or its subcontractors will make any press or public statements regarding the services they provide or the information they access?

Guidance: If so, the agreement should include a statement explaining that the contractor or its subcontractors must notify the Agency about any press statement or publication related to the services or information.

Sample Language: If Contractor plans to issue any public statement, press release, or other publication in any media format regarding the services or information shared under this Agreement, it must send Agency written notice at least one week before issuing the anticipated statement.

The Contractor, and its officers, employees, and agents shall notify the Agency, at any time either during or after completion or termination of this Agreement, of any intended statement to the press or any intended issuing of any material for publication in any medium of communication (print, news, television, radio, Internet, etc.) regarding the services provided or the data collected pursuant to this Agreement at least 72 hours prior to any statement to the press, or at least five business days prior to the submission of the material for publication, or such shorter periods as are reasonable under the circumstances. The Contractor may not issue any statement or submit any material for publication that includes Sensitive Identifying Information or information otherwise designated as confidential under this Agreement.

7. Prohibition on the Sale or Monetization of Sensitive Identifying Information

Question: Will the contractor or its subcontractors seek to sell or monetize Sensitive Identifying Information, whether by direct request or as part of its general business model, policies and practices?

Guidance: Agencies' agreements with contractors, pursuant to which the contractor has access to Sensitive Identifying Information provided by the City or otherwise made available to the contractor in connection with the agreement, must include language prohibiting the contractor from selling or otherwise using or disclosing the Sensitive Identifying Information for the contractor's financial benefit or other business need unless expressly authorized under the agreement.

Sample language: Except as otherwise provided in this Agreement, Contractor shall only use Sensitive Identifying Information for the purposes set forth in this Agreement, and shall not disclose such information to any third parties, except as required by law. In addition, Contractor shall not use Sensitive Identifying Information for the benefit of another individual or entity, or publish, sell, monetize, license, distribute, or otherwise reveal such information.