NYC OTI
Office of Technology & Innovation

Citywide Privacy Protection Policies and Protocols

January 28, 2025

Version 4.0

Page Intentionally Blank

VERSION CONTROL

Version	Description of Change	Approver	Date
4.0	Enhanced definitions of sensitive identifying information, biometric information, consent, and Artificial Intelligence and AI Systems. Added guidance for privacy impact assessments, contextual integrity, privacy-enhancing techniques and technologies, privacy by design, and program-specific privacy policies. Added supplemental guidance on disclosures involving the New York City Police Department and the Department of Investigation. Added new guidance for offerings of identity protection services, and receiving complaints from the public. Revised requirements for requesting deviations from the standard text of the Identifying Information Rider and requesting best interests of the city determinations. Revised Identifying Information Law quarterly report due dates. Added height and weight, and designated shelter address, mental or physical condition, prescriptions, diagnoses, medical history, healthcare policy number, case identifiers, and case disposition as new types of identifying information and updated Identifying Information Table.	Michael Fitzpatrick Chief Privacy Officer, City of New York	1/28/2025
3.0	Updated Privacy Principles. Added explanation of the City's data breach notification law. Included additional terms not defined in the Identifying Information Law. Added descriptions of key agency executive roles with which agency privacy officers should cooperate. Added references to the revised Agency Privacy Officer Toolkit. Added explanation of contextual integrity of identifying information to guide APO decision-making for approvals. Added references to OIP's citywide privacy training and Office of Cyber Command's cybersecurity awareness training. Added requirement for agency privacy officers to notify the Chief Privacy Officer of collections and disclosures under exigent circumstances or in violation of the Identifying Information law within 24 hours of discovery.	Michael Fitzpatrick Chief Privacy Officer, City of New York	2/6/2023

	Made stylistic edits throughout and added subheadings for clarity and ease of reading. Appendix items on contracts moved to the revised Agency Privacy Officer Toolkit. Hyperlinked to all external documents where mentioned. Hyperlinked to sections of the Policy where referenced.		
2.1	Updated logo to reflect the Office of Information Privacy's reorganization into the Office of Technology and Innovation. Updated uses of "Mayor's Office of Information Privacy" and "DoITT" to "Office of Information Privacy" and "OTI," respectively, pursuant to Executive Order 3 of 2022. Updated the Chief Privacy Officer's name to reflect current appointee. Updated hyperlinks to reflect website revisions.	Michael Fitzpatrick Chief Privacy Officer, City of New York	10/6/2022
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

Page Intentionally Blank

Office of Technology & Innovation

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

Table of Contents

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 collections, uses, disclosures, access to, and retentions of identifying information by City agencies and certain City contractors and subcontractors.

1.2 Authority

The Chief Privacy Officer's power to issue this Policy comes from **New York City Charter 8(h)** and **Administrative Code of City of NY §§ 23-1201 through 23-1205**, which together form the **Identifying Information Law**.

The Policy is informed by the Identifying Information Law's requirements and by the Citywide Privacy Protection Committee's recommendations.[1]

1.3 Applicability

This Policy applies to all City agencies except the ones listed in **Appendix A**. Covered City agencies must comply with this Policy. Agency contractors and subcontractors providing services designated in **Section 6.1** of this Policy (**covered contractors and subcontractors**) must also comply with this Policy.

The Chief Privacy Officer encourages agencies not covered by this Policy to review and follow the Identifying Information Law and this Policy, in whole or in part.

Agency privacy officers have key responsibilities for carrying out the requirements of the Identifying Information Law and this Policy. Compliance at the agency level is, however, ultimately the responsibility of agency heads. Agency privacy officers should seek guidance from the Chief Privacy Officer to help their agencies follow the Identifying Information Law and this Policy.

1.4 Modification

This Policy may be amended by the Chief Privacy Officer to address other requirements and best practices for collecting, using, disclosing, accessing, and retaining identifying information. The Chief Privacy Officer will notify agency privacy officers when this Policy is amended.

[1] The Citywide Privacy Protection Committee is the committee required by Admin. Code § 23-1204.

1.5 Relationship to Other City and Agency Policies

1.5.1 Executive Order No. 3 of 2022

Executive Order No. 3 of 2022 recognizes the City's commitment to improving the coordination of City resources and services across agencies to ensure the efficient, safe, and timely delivery of services to residents and communities. This Policy sets forth requirements and provides information on data privacy and security protections to facilitate responsible data sharing to further important City and cross-agency collaborations and initiatives.

1.5.2 Agency Privacy Policies, Protocols, and Practices

This Policy is the baseline requirement for City agencies relating to collections, uses, disclosures, access to, and retentions of identifying information. City agencies may adopt supplemental policies that address their unique needs or laws governing the identifying information they collect, use, access, disclose, or retain.

Agency privacy officers must issue guidance to their agencies' employees, and to covered contractors and subcontractors, on their agencies' collections, uses, disclosures, access to, and retentions of identifying information. Refer to Section 4.2 of this Policy for more information on agency privacy officer responsibilities and related guidance.

> ➢ **Guidance Tip:** Develop relationships with records access officers, chief information security officers, agency chief contracting officers, and others, to stay up to date on agency and citywide developments. Refer to Section 4.2.3.1 for descriptions of these key executive roles.

1.5.3 Citywide Cybersecurity Program Policies and Standards

The Citywide Cybersecurity Program Policies & Standards and Citywide Technology Policies and Guidelines are issued by the New York City Office of Technology and Innovation through its Office of Cyber Command (**Cyber Command**). These policies regulate how agencies classify, transfer, and store information. The following policies are especially relevant to properly handling and protecting identifying information:

- Citywide Data Classification Policy
- Citywide Data Classification Standard
- Citywide Information Management Policy
- Citywide Information Management Standard
- Citywide Cybersecurity Categorization of Data and System Policy
- Citywide Cybersecurity Categorization of Data and System Standard
- Citywide Cybersecurity Categorization of Data and System Guidance
- Citywide Inventory Policy
- Citywide Multi-Factor Authentication Policy
- Citywide Multi-Factor Authentication Standard
- Citywide Encryption Policy
- Citywide Encryption Standard
- Citywide Cybersecurity Requirement for the Reuse and Disposal of Systems and Non-Computing Storage Devices Policy
- Citywide Cybersecurity Requirement for the Re-use and Disposal of Systems and Non-Computing Storage Devices Standard
- Mobile Computing Device Security Policy
- Portable Data Security Policy
- Citywide Incident Response Policy
- Citywide Cloud Policy
- User Responsibilities Security Policy
- Citywide Cybersecurity Control of System Policy

1.5.3.1 Agency Privacy Officer Role in Ensuring Compliance with Citywide Information Technology and Security Policies and Standards

Agency privacy officers should coordinate with their information technology units, their general counsel's office, their agency chief information security officer, and Cyber Command to identify and address the impact of technical requirements for their agencies' collections, uses, disclosures, access to, and retentions of identifying information. They should also identify agency-specific information technology and security policies[2] and incorporate relevant sections of the Citywide Cybersecurity Program Policies and Standards, Citywide Technology Policies and Guidelines, agency-specific information technology and security policies, and guidance from information technology leadership and Cyber Command in guidance they issue. The Chief Privacy Officer will distribute security guidance from Cyber Command to agency privacy officers.

Refer to **Section 6.0** for guidance on incorporating privacy- and security-related attachments into agreements.

> ➢ **Guidance Tip:** Raise questions about privacy and security directly to the Chief Privacy Officer at **oip@oti.nyc.gov** or at a **meeting with the Chief Privacy Officer**.

1.5.4 Mayoral Directive 2015-3: Uniform Records Management Practices

City agencies must keep identifying information when required by law or to further the mission or purpose of the agency. They may also keep identifying information when retaining it is in the interests of the City, is not contrary to the purpose or mission of the agency, and is otherwise permitted by law.[3] Complying with **Mayoral Directive 2015-3**, which sets forth the City's Uniform Records Management Practices, is in the interests of the City. Agencies must comply with information retention requirements, including the agency's Records Retention and Disposition Schedule approved by the Department of Records and Information Services. Refer to **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**).[4] The Model Protocols set forth a factual and legal assessment process that agencies must follow when a third party asks for City information, including identifying information. Agencies must either adopt the Model Protocols or adopt comparable protocols.

1.5.6 General Confidentiality Policy

Executive Order Numbers 34 and **41** of 2003 (the **General Confidentiality Policy**) regulate the collection and disclosure of certain identifying information designated as "confidential." Specifically, the General Confidentiality Policy regulates the disclosure of "any information obtained and maintained by a City agency relating to an

[2] Relevant agency-specific policies may include acceptable use policies, acceptable email usage policies, IT and equipment policies, and remote access policies, or other policies that address employees' use of City- or agency-issued devices or use of personal devices or email addresses for City business.
[3] *See* Admin. Code § 23-1202(e).
[4] 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.

individual's sexual orientation, status as a victim of domestic violence, status as a victim of sexual assault, status as a crime witness, receipt of public assistance, or immigration status [and] all information contained in any individual's income tax records." The General Confidentiality Policy also prohibits inquiring about a person's immigration status unless an exception applies.

The General Confidentiality Policy is consistent with the Identifying Information Law and this Policy. Together, they create a comprehensive, citywide framework for privacy protection and best practices by City agencies for the collection and disclosure of New Yorkers' identifying information.

1.6 Relationship of the Identifying Information Law to Other Laws

Where a federal or state law or regulation conflicts with the Identifying Information Law, the federal or state law or regulation governs. 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**) allows the public to ask for copies of government records and requires City agencies to disclose records unless an exemption applies.[5] These records may include identifying information.

When the Freedom of Information Law, a state law, requires an agency to disclose identifying information, the agency must disclose it, and the agency privacy officer should approve the disclosure as required by law.[6]

If the Freedom of Information Law does not require an agency to disclose identifying information because an exemption applies, such as where the disclosure would constitute an unwarranted invasion of personal privacy, the agency may only disclose the identifying information if its agency privacy officer determines that the disclosure furthers the purpose or mission of the agency.[7]

1.6.1.1 Publishing FOIL Request Titles on the Open Records Portal

People may submit Freedom of Information Law requests by contacting a City agency directly or by submitting a request through the City's Freedom of Information Law portal (**OpenRecords Portal**), which is managed by the Department of Records and Information Services.[8] The OpenRecords Portal displays certain information about every Freedom of Information Law request placed on the OpenRecords Portal, including the title created for it by the person who submitted the request.[9] The request title may contain identifying information. When an agency receives a Freedom of Information Law request via the OpenRecords Portal, it should determine whether the title

[5] *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).
[6] *See* Admin. Code § 23-1202(c)(1)(c).
[7] *See* Admin. Code § 23-1202(c)(1)(b).
[8] 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.
[9] 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.

of the request contains any identifying information that should not be publicly disclosed on the OpenRecords Portal (such as Social Security numbers).

To give records access officers time to make this determination in consultation with their agency privacy officer, the OpenRecords Portal withholds Freedom of Information Law request titles from publication on the OpenRecords Portal for five business days. This delay purposefully coincides with the Freedom of Information Law's "acknowledgement period."[10] Agencies must determine whether to redact identifying information contained in the Freedom of Information Law request title within this five-day period.

- **Guidance Tip:** Each agency subject to the Freedom of Information Law has a records access officer 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 Freedom of Information Law request where disclosure is not mandatory under the Freedom of Information Law, and a Freedom of Information Law exemption is available, but the agency is considering whether to disclose the information voluntarily. See "**Guidance on the City's Identifying Information Law in Relation to Open Data**" for more information.

1.6.2 Open Data Law

New York City's **Open Data Law** makes all "public data sets"[11] available online through a single web portal (**Open Data Portal**). Each agency has an open data coordinator responsible for publishing public data sets.

Some data sets contain identifying information. The definition of "public data set" excludes information that *any* law exempts from disclosure.[12] Agency privacy officers are responsible for determining whether identifying information constitutes a "public data set." Agency privacy officers should consult with their open data coordinators to determine whether the agency's public data sets include identifying information before a data set is published on the Open Data Portal.

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

1.6.3 Administrative Code 10-501 – 10-504 (Agency Disclosures of Security Breaches)

Admin. Code §§ 10-501 to 10-504 set out requirements for City agencies following "the unauthorized access, acquisition, disclosure or use of computerized data that compromises the security, confidentiality or integrity of private information maintained by an agency."[13] Admin. Code § 10-502 requires any city agency to notify the Chief Privacy Officer and Cyber Command if a breach of the agency's security has occurred where an individual's

[10] N.Y. Pub. O. Law § 89(3)(a) grants entities subject to FOIL five business days to acknowledge receipt of a FOIL request.
[11] *See* Admin. Code § 23-501(g).
[12] *Id.*
[13] *See* Admin. Code §§ 10-501(c).

personal information has been, or is reasonably believed to have been, accessed, acquired, disclosed, or used without authorization. Refer to **Section 4.4.1** for more information on unauthorized disclosures.

2.0 Privacy Principles

In providing services and resources, the City of New York often collects, uses, discloses, accesses, or retains identifying information across agencies and with other parties. The City protects the identifying information it keeps about its employees, officials, and the public.

Agencies should follow the City's **Privacy Principles** to enable privacy protection and responsible handling of identifying information.

The Privacy Principles are values underlying agency practices, and agencies should honor them in all aspects of their decision-making and operations. They should be referenced when developing partnerships with private entities, providing programs and services, in agency rulemaking, developing technical systems and solutions, and engaging in other policy and decision-making that may affect privacy.

Agencies should use the **Privacy Impact Assessment** in the **Agency Privacy Officer Toolkit** to help implement the Privacy Principles while designing their projects.

	Privacy Principle	Description
1	Transparency	City agencies must clearly inform the public about how and why they collect, use, disclose, access, and retain identifying information, as well as give people the opportunity to make choices about their identifying information, when possible.
2	Public Trust	City agencies must collect identifying information lawfully and fairly and, when possible, directly from people with their knowledge and consent. Agencies should publicly share details about their privacy practices and handling of identifying information, where appropriate.
3	Accountability	City agencies must implement privacy practices, and periodically assess, audit, and modify them as necessary to keep pace with privacy and security threats and standards and best practices.
4	Data Minimization	City agencies must collect, use, disclose, access, and retain identifying information only as necessary for an articulated and legally permissible purpose and utilizing the minimum necessary data elements for the stated purpose.
5	Use Limitation	City agencies must articulate the specific need for each collection, use, disclosure, access to, or retention of identifying information, including the legal authority and agency purpose, and only use identifying information in ways compatible with the purpose of the collection.
6	Responsible Governance and Stewardship	City agencies must protect identifying information and should collect, use, disclose, access, and retain identifying information only through authorized persons for authorized purposes.
7	Data Quality, Integrity, and Accuracy	City agencies must protect the quality, integrity, and accuracy of identifying information and take reasonable steps to correct, update, or securely dispose of inaccurate or outdated identifying information. City agencies should allow individuals to access and correct their identifying information when appropriate, as well as consider the context in which data elements are collected, used, disclosed, accessed, and retained.
8	Security Safeguards	City agencies must use appropriate physical and digital safeguards to protect identifying information from threats and from unauthorized collection, use, disclosure, access, and retention and follow current privacy and security best practices and standards.
9	Equity	City agencies must consider equity in privacy protection and discourage, mitigate, and protect against discrimination, misuse, and exploitation in the collection, use, disclosure, access to, or retention of identifying information.

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.[14] The Identifying Information Law has a partial list of types of information and authorizes the Chief Privacy Officer to designate additional types of information. The list of types of identifying information is non-exhaustive. Agencies must protect any information that alone or in combination with other information could identify or locate an individual.

Enumerated Types of Identifying Information:	
Personal Information Name Social Security number (full or last 4 digits)* Taxpayer ID number (full or last 4 digits)*	**Work-Related Information** Employer information Employment address
Biometric Information Fingerprints Photographs Height† Weight† Palm and handprints* Retina and iris patterns* Facial geometry* Gait or movement patterns* Voiceprints* DNA sequences*	**Government Program Information** 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 Shelter address*
Contact Information Current and/or previous home addresses Email address Phone number	**Health Information** Mental or physical condition* Prescriptions* Diagnoses* Medical history* Healthcare policy number*
Demographic Information Country of origin Date of birth* Gender identity Languages spoken Marital or partnership status Nationality Race Religion Sexual orientation	**Public Safety** Arrest record or criminal conviction Case identifiers* Case disposition* Date or time of release from custody Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD

[14] *See* Admin. Code § 23-1201.
† Types of identifying information added by Local Law 61 of 2023.
* Types of identifying information designated by the Chief Privacy Officer.

Enumerated Types of Identifying Information:	
Status Information	**Technology-Related Information**
Citizenship or immigration status Employment status Status as victim of domestic violence or sexual assault Status as crime victim or witness	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 Guidance in Determining When Other Information Constitutes Identifying Information

The Identifying Information Law explicitly applies to "identifying information" listed in Admin. Code § 23-1201 or designated by the Chief Privacy Officer. The Identifying Information Law may also apply to other information depending on the context, or facts and circumstances in which the information is being collected or disclosed. Refer to Section 3.2.8 for information regarding contextual integrity and how to evaluate the contextual integrity of information.

When deciding whether particular information can by itself or in combination with other information identify or locate a person, agency privacy officers should consider a variety of factors including the type and volume of data elements, their current, real-world availability, and which data elements can reasonably be expected to be published in the future. Generally, the more data elements that can be strung together, the more likely it is that a person can be identified or located.

For example, "zip code" is a data element that might be identifying in some contexts and not in others, especially as different zip codes contain vastly different numbers of people. In a data analytics project, if fewer than five individuals meeting program criteria live within one zip code, it is more likely that zip code should be considered identifying. If other information is also available about individuals, like program affiliation or other physical descriptors, then zip code 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 Access

"Access" means gaining the ability to read, use, copy, modify, process, or delete any information, whether or not by automated means.

3.2.2 Artificial Intelligence and AI System

"Artificial Intelligence" and "AI System" mean a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract

* Types of Identifying Information designated by the Chief Privacy Officer.

such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.[15]

3.2.3 Anonymized

"Anonymized" means having minimized or removed the elements of information that identify an individual. Anonymization is part of a broader category of privacy-enhancing techniques and technologies. Refer to **Section 5.6** for additional guidance on privacy-enhancing techniques and technologies.

3.2.4 Biometric Information

"Biometric information" means any information that is based on measurements of physical or behavioral characteristics of an individual that may be used on its own or with other information to identify or locate an individual.

3.2.5 Collection

"Collection" means an action to receive, retrieve, extract, or access identifying information. Collection does not include receiving information that an agency did not ask for.

Collection does not include acting only as a technical conduit for identifying information. For example, an agency providing Internet service receives the identifying information that passes through its service but does not "collect" it. This exception applies to very few agency functions.

3.2.6 Complaint

"Complaint" means a notification about a suspected or known violation of the Identifying Information Law. The Identifying Information Law does not create a private right of action,[16] but agencies must have a process for receiving and investigating complaints.[17]

3.2.7 Consent

"Consent" means a freely given, specific, informed, and unambiguous indication of an individual's agreement to the collection, use, or disclosure of the individual's identifying information.

3.2.8 Contextual Integrity

"Contextual integrity" means the context, actors, attributes, and transmission principles associated with identifying information. Refer to **Section 4.3** for additional information about contextual integrity.

[15] *See* Artificial Intelligence: Principles and Definitions.
[16] Admin. Code § 23-1202(h).
[17] Admin. Code § 23-1203(9).

3.2.9 Disclosure

"Disclosure" means releasing, transferring, disseminating, giving access to, or otherwise providing identifying information in any manner outside the agency. Disclosure includes accidentally releasing information and access to identifying information obtained through a potential unauthorized access to an agency's systems or records.

Disclosure does not include acting only as a technical conduit for identifying information. For example, an agency providing Internet service releases the identifying information that passes through its service but does not "disclose" it. This exception applies to very few agency functions.

3.2.10 Exigent Circumstances

"Exigent circumstances" means cases where following this Policy would cause undue delays. Refer to **Section 5.4** for detailed guidance on exigent circumstances.

3.2.11 Sensitive Identifying Information

"Sensitive identifying information" means identifying information that poses a higher risk of harm to an individual or members of an individual's household. Examples of harm are identity theft, danger to health and safety, severe financial loss, reputational harm, or other harms dependent upon any protected status of an individual.

Identifying information can be "sensitive identifying information" by its very nature or under specific circumstances. For example, sensitive identifying information can include patterns of life, habits, and potentially sensitive activities and locations associated with an individual. This may encompass regular routines, frequented places, or recurring behaviors that, when combined or analyzed, could reveal private aspects of an individual's life or expose them to potential harm if disclosed. Agency privacy officers or the Chief Privacy Officer determine when identifying information is "sensitive identifying information."

3.2.11.1 Requirements When Handling Sensitive Identifying Information

Sensitive identifying information is classified as "Restricted" information under the Citywide Data Classification Standard and must be handled in accordance with the Citywide Information Management Standard. Refer to **Section 3.1** for the definition of "identifying information," **Section 5.5** for requirements for requests and proposals involving sensitive identifying information, and the **Agency Privacy Officer Toolkit** for guidance on protecting sensitive identifying information in relevant provisions of contracts.

3.2.12 "Requests" for Identifying Information

"Requests" for identifying information[18] means third-party requests for identifying information. Examples of "requests" are press or media inquiries, FOIL requests, subpoenas, requests from another agency, requests from elected officials for oversight purposes, or information that is available to the public pursuant to the Open Data Law.

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

[18] *See* Admin. Code § 23-1205(a)(1)(c)(1).

3.2.13 "Proposals" for Identifying Information

"Proposals" for identifying information[19] means requests for identifying information for specific projects. Examples of "proposals" are projects for data integration, analysis, research, or other initiatives that involve sharing identifying information across agencies or with outside entities for a particular proposed project.

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

3.2.14 Use

"Use" of identifying information means any operation performed on identifying information, whether or not by automated means, such as collection, storage, transmission, consultation, retrieval, disclosure, or destruction.

4.0 Agency Privacy Officer

4.1 Designation

Each agency head must designate a privacy officer.[20] Agencies must promptly notify the Chief Privacy Officer of the name and contact information for any new privacy officer and impending vacancy of their position by emailing **oip@oti.nyc.gov**. If an agency privacy officer relinquishes the position, they must promptly notify the agency head so the agency head can designate a new agency privacy officer as soon as practicable.

4.1.1 Agency Employee Designations

The designation of an agency privacy officer is a significant decision for the agency. Agency privacy officers should have fluency with agency privacy policies and practices, knowledge of current legislative, regulatory, and policy developments relating to privacy protection, and strong communication and collaboration skills.

Agency heads or their designees should consult the Chief Privacy Officer before newly designating agency privacy officers. The Chief Privacy Officer will advise the agency head[21] on necessary technical, legal, and cross-functional skills the agency privacy officer should possess, incorporating the agency's specific privacy needs.

> ➢ **Guidance Tip:** The Chief Privacy Officer can assist agencies with drafting job descriptions for privacy-related openings, advertising and promoting openings, and interviewing final candidates.

The Chief Privacy Officer strongly recommends that agency privacy officers be attorneys when possible. Agency privacy officers who are not attorneys should consult with their agency's general counsel, the Chief Privacy Officer, or the City's Law Department before making legal decisions.

[19] *See* Admin. Code § 23-1205(a)(1)(c)(2).
[20] *See* Admin. Code § 23-1201.
[21] NYC Charter § 8(h)(5).

4.1.1.1 Records Access Officer

Agency records access officers may act as agency privacy officers when a third party asks for identifying information as part of a Freedom of Information Law request.[22] Refer to **Section 1.6.1** on the relationship of the Freedom of Information Law to the Identifying Information Law.

4.1.2 Contractors and Subcontractors

Agencies may let a covered contractor or subcontractor act as the agency privacy officer for a specific contract or subcontract.[23] The covered contractor or subcontractor will be responsible for the privacy officer functions described in **Section 4.2**.

4.1.3 Agency Privacy Officer Training

The Office of Information Privacy provides remote training sessions for newly designated agency privacy officers. These sessions explain the basics of the Identifying Information Law and agency privacy officers' responsibilities under the Identifying Information Law and this Policy. The Office of Information Privacy schedules sessions after being informed that an agency has newly designated a privacy officer, but new designees may also request a session by **self-scheduling** or by emailing **oip@oti.nyc.gov.** Refresher training on these topics is also available for current agency privacy officers.

4.2 Agency Privacy Officer Responsibilities

4.2.1 Agency Privacy Protection Policies and Guidance

Agency privacy officers must compile and report certain information about agencies' collection, use, disclosure, access to, and retention of identifying information. Agency privacy officers must adopt this Policy as a baseline for protecting identifying information, and for compiling and reporting[24] information about their policies.

Agency privacy officers must inform agency employees and covered contractors and subcontractors about this Policy and the Identifying Information Law.[25] Agency privacy officers may also issue agency-specific policies that build on this Policy.

4.2.2 Agency Compliance Plan

Agency privacy officers must develop a plan for following the Identifying Information Law and this Policy.[26] The **Agency Privacy Officer Toolkit** contains model compliance plans and guidance that agency privacy officers can adopt or adapt. The Toolkit contains tools for agency privacy officers to assess and improve their internal compliance processes.

[22] *See* Admin. Code § 23-1201.
[23] *See* Admin. Code § 23-1202(g).
[24] *See* Admin. Code § 23-1205.
[25] *See* Admin. Code § 23-1203(2).
[26] *See* Admin. Code § 23-1203(8).

4.2.3 Agency Liaison Network

Agency privacy officers should establish working relationships with key executives and business units within their agencies. Developing robust internal networks helps agency privacy officers understand their agencies' work as it changes over time. Agency privacy officers should have ongoing conversations with their agencies' chief information security officers and general counsels, at minimum, to better coordinate on privacy, security, risk management, incident response, and other areas of responsibility.

4.2.3.1 Descriptions of Key Agency Executive Roles

Key agency executives that agency privacy officers should coordinate with in performing their duties include:

Chief Information Security Officer: an agency's chief information security officer is responsible for implementing their agency's cybersecurity program under the guidance of Cyber Command and ensuring that the program is consistent with citywide cybersecurity standards. Since cybersecurity is crucial for protecting privacy, agency privacy officers must have a close working relationship with their agency's chief information security officer, especially in cases of potential security incidents or unauthorized disclosures of identifying information.

Chief Contracting Officer: the duties of an agency's chief contracting officer include overseeing the coordination, planning, and implementation of their agency's contract and procurement activities, overseeing vendor responsibility and performance, and general advising on procurement matters. Agency privacy officers should work closely with chief contracting officers on issues such as vendor compliance with the Identifying Information Law and other privacy laws as well as privacy evaluations of vendor products.

General Counsel: an agency's general counsel is responsible for overseeing all agency legal matters. Non-attorney agency privacy officers *must* have a working relationship with agency counsel due to the legal nature of an agency privacy officer's duties, but all agency privacy officers should work closely with agency counsel because privacy issues can arise in any legal context (e.g., contracts, litigation, or employment matters).

Agency Personnel Officer: an agency personnel officer is responsible for managing all aspects of human resources, including recruitment, hiring, employee relations, performance evaluations, disciplinary actions, and benefits administration. Agency privacy officers should be familiar with their agency personnel officers and work closely with them on human resources-related collections and disclosures of identifying information.

4.2.4 Agency Privacy Officer Toolkit

The **Agency Privacy Officer Toolkit** is a comprehensive resource for agency privacy officers to implement the requirements of the Identifying Information Law and this Policy. It contains a model Identifying Information Law compliance plan, model guidance and reference documents, a model investigation plan, and guidance for contracts and agreements.

Many of the materials contained within the **Agency Privacy Officer Toolkit** are available on the **Office of Information Privacy's intranet page**, along with supplemental and annotated documents.

4.3 Approval of Collections and Disclosures

Agency privacy officers must consider context, actors, attributes, and transmission principles, referred to as contextual integrity (Refer to **Section 3.2.8**), when approving collections and disclosures by aligning the

collections, disclosures, and uses of identifying information with their agency norms, legal requirements, purposes, and expectations. The **Agency Privacy Officer Toolkit** contains detailed guidance on considering contextual integrity.

Context is the legal, factual, and social backdrop informing how identifying information should be handled. Examples include law enforcement, health care, or social services. Each context has unique norms and legal standards. Agency privacy officers should consider both broader larger contexts (such as health care) and sub-contexts (physician interactions versus insurance processing). Agency privacy officers may define norms when appropriate.

Actors are the sender, recipient, and subject of identifying information. Agency privacy officers should identify the actors and their associated obligations and expectations about who accesses identifying information, under what conditions, and for what purposes.

Attributes are the characteristics of identifying information. Agency privacy officers should balance the level of detail to protect privacy while meeting the agency's operational needs by identifying the minimum amount of identifying information necessary to accomplish the agency's articulated business purposes. Agency privacy officers should obtain this information from the actors or other stakeholders.

Transmission principles are the rules, norms, and expectations governing how information is collected or disclosed.

> ➢ **Guidance Tip:** Consider whether people would be surprised to know how their identifying information is being collected, used, disclosed, or accessed.

4.3.1 Privacy by Design

Agencies are encouraged to use privacy by design processes in the development of any agency system, application, or service that processes identifying information. Privacy by design is a collaborative process that embeds privacy protections directly into the foundational architecture of technologies, systems, and business processes at the earliest stages of the project lifecycle. The **Agency Privacy Officer Toolkit** offers detailed guidance on how to implement privacy by design.

Privacy by design generally involves that privacy-related measures that are enabled by default, meaning that projects are designed to collect, use, and disclose the minimum amount of identifying information required for the project's purpose while providing users with the level of privacy protection and decision-making capabilities appropriate to the context. Agencies must also classify identifying information during the privacy by design process under the Citywide Information Management Standard, which provides security requirements based on the classification.

> ➢ **Guidance Tip:** To determine the appropriate level of privacy protection, analyze the contextual integrity (refer to **Section 3.2.8**) of the identifying information to be processed, consider the City Privacy Principles (refer to **Section 2.0**), and evaluate the costs, risks, and benefits of implementing related privacy-enhancing techniques and technologies. Agencies should also consider completing a Privacy Impact Assessment before implementing a new project involving identifying information or changing how an existing project handles identifying information. Refer to **Section 5.6** for guidance on privacy-enhancing techniques and technologies and the **Agency Privacy Officer Toolkit** for the Privacy Impact Assessment.

4.3.2 Individual Consent

The Identifying Information Law permits the agency privacy officer to approve disclosure of identifying information when required by law, when such disclosure furthers the agency's mission or purpose, or when an agency obtains written authorization from the individual to whom the information pertains, or from their parent or guardian, or other person with legal authority to consent on behalf of the individual.[27] Agency privacy officers may thus approve the disclosure of identifying information for which consent has been obtained even if the disclosure is not required by law and does not further an agency's mission or purpose.

> ➢ **Guidance Tip:** Agency privacy officer approval is required even when consent has been obtained. The agency privacy officer may approve such disclosures as routine.

Agencies should consider whether to obtain individual consent before collecting identifying information (refer to **Section 2.0** "Public Trust") and before using or disclosing identifying information (refer to **Section 3.2.14** for the definition of "use"). Some laws may require consent to be obtained in specific ways when collecting, using, or disclosing identifying information in specific contexts. Agency privacy officers should consider the contextual integrity of the identifying information (refer to **Section 3.2.8**) when determining the appropriate type and scope of consent.

> ➢ **Guidance Tip:** The best practice is to incorporate individual consent unless there are articulable reasons why consent is impracticable or inappropriate.

All consent obtained for the collection, use, or disclosure of identifying information should meet the definition in this Policy (refer to **Section 3.2.7**). When obtaining consent, agencies should typically explain:

- The types of identifying information involved.
- The entities that will collect, use, or disclose the identifying information.
- The purpose and scope of the collection, use, or disclosure.
- The legal basis for the collection, use, or disclosure.
- How long the identifying information will be retained.
- That an individual may refuse or withdraw consent at any time.
- Any consequences of withholding consent.
- Whether the agency will continue to use or disclose identifying information collected before consent was withdrawn.

> ➢ **Guidance Tip:** Refer to the **Agency Privacy Officer Toolkit** for sample consent forms. Agency privacy officers may also consult the Chief Privacy Officer for assistance on the type and scope of appropriate consent for a given project.

4.3.3 Pre-approval as Routine

Agency privacy officers may pre-approve collections or disclosures of identifying information as "routine."[28] "Routine" approvals are necessary because agencies collect and disclose identifying information in their normal

[27] Admin. Code § 23-1202(c)(1)(a).
[28] *See* Admin. Code §§ 23-1202(b)(2)(a) and (c)(2)(a).

business operations. These designations allow those collections and disclosures to continue lawfully 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 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.

4.3.4 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.[29] Agency privacy officers may also approve disclosures if an individual, or a guardian or other person with legal authority to consent on behalf of an individual, has consented. Case-by-case approvals must be documented by the agency privacy officer and sent to agency staff and covered contractors and subcontractors operating under their approval. Examples of case-by-case approvals include unique data integration projects, analytics or research projects, or press inquiries.

> ➢ **Guidance Tip:** Agency privacy officers should give special attention to online analytics, which may manifest when using tracking pixels on agency- or contractor-operated websites. Refer to the Agency Privacy Officer Toolkit for detailed guidance regarding online analytics.

Unless exigent circumstances exist, agencies must obtain approval from their agency privacy officers for collections or disclosures that have not been designated as "routine."

Agency privacy officers may designate collections or disclosures as "routine" or on a case-by-case basis at any time. Agency privacy officers may also redesignate collections and disclosures from "routine" to case-by-case or from case-by-case to "routine," and may change the content of their designations at any time.

4.3.5 Exemptions for Collections or Disclosures

The Identifying Information Law prohibits unapproved collections or disclosures of identifying information. There are two exemptions.

4.3.5.1 Exemption for Collections or Disclosures Involving Police Investigations

No agency privacy officer approval is needed when 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.[30]

[29] *See* Admin. Code §§ 23-1202(b)(1) and (c)(1).
[30] *See* Admin. Code §§ 23-1202(b)(2)(c)(1) and (c)(2)(c)(1).

Agency privacy officers who are consulted with respect to disclosures to the New York City Police Department should accept the New York City Police Department's assertion that the disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime.

> **Guidance Tip:** Agencies and the New York City Police Department may choose to enter into data sharing agreements for disclosures of identifying information to the Department in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime.

4.3.5.2 Exemption for Collections or Disclosures Involving Child Welfare Investigations or Investigations Relating to Individuals Who are Not Legally Competent

No agency privacy officer approval is needed when identifying information is collected or disclosed 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.[31]

4.4 Reporting

4.4.1 Agency Reports

Agencies must report detailed information about their collections or disclosures of identifying information and about their privacy practices. The reports are due by July 31 in even-numbered years and are submitted to the Mayor, the Speaker of the City Council, the Chief Privacy Officer, and the Citywide Privacy Protection Committee.[32] Agency privacy officers should work with agency heads and general counsels to comply with this obligation. Agencies are free to report more information than required by the Identifying Information Law.

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

Agency privacy officers are responsible for gathering information on any unauthorized disclosures or any collections or disclosures made under exigent circumstances. Agency privacy officers must notify the Chief Privacy Officer of this information as soon as practicable,[33] which means within 24 hours of learning of the unauthorized disclosure or collections or disclosures made under exigent circumstances.

The Chief Privacy Officer creates and submits quarterly anonymized summaries of agencies' reports to the Speaker of the Council,[34] and makes them available **online**.[35] The quarters run as follows: January 1st through March 31st (1st Quarter); April 1st through June 30th (2nd Quarter); July 1st through September 30th (3rd Quarter); and October 1st through December 31st (4th Quarter).

[31] *See* Admin. Code §§ 23-1202(b)(2)(c)(2) and (c)(2)(c)(2).
[32] *See* Admin. Code § 23-1205.
[33] Admin. Code §§ 23-1202(c)(4) and (d)(1).
[34] *See* Admin. Code §§ 23-1202(c)(4) and (d)(2).
[35] *Id.*

4.4.2.1 Timing of Reporting Unauthorized Disclosures or Collections and Disclosures Made Under Exigent Circumstances

The Chief Privacy Officer issues reminders to all agency privacy officers near the close of each quarter to report unauthorized disclosures and collections or disclosures made under exigent circumstances. Nevertheless, agency privacy officers must notify the Chief Privacy Officer within 24 hours of discovery when an individual's identifying information is either disclosed without agency privacy officer authorization, or collected or disclosed under exigent circumstances, even if the Chief Privacy Officer's report is not yet due.[36] Agency privacy officers should also notify the agency's general counsel of any suspected or known unauthorize. Refer to **Section 8.0** for information on receiving and investigating complaints for violations of the Identifying Information Law.

> ➢ **Guidance Tip:** The purpose of notifying the Chief Privacy Officer within 24 hours is to allow the Chief Privacy Officer and Office of Information Privacy to support the agency privacy officer and agency in investigating and remediating. Submitting a prompt notification enables the Chief Privacy Officer and Office of Information Privacy to provide this support as rapidly as possible.

The agency may not have complete information about the unauthorized collection or disclosure or disclosure under exigent circumstances at the time it notifies the Chief Privacy Officer. The notification should nevertheless be sent to the Chief Privacy Officer with enough information to apprise the Chief Privacy Officer. Agency privacy officers must use the form prescribed by the Chief Privacy Officer unless the circumstances make it impractical to do so or would unreasonably delay notification. If an agency privacy officer uses a non-prescribed notification method, the agency privacy officer must follow up that notification with the prescribed notification method.

4.5 Participation in Committees and Working Groups

The Chief Privacy Officer may invite agency privacy officers, or others, to participate in committees or working groups. These groups support the Chief Privacy Officer's consideration of cross-agency privacy matters, policy development, or specific operational challenges requiring collective expertise.

4.5.1 Citywide Privacy Protection Committee

The Citywide Privacy Protection Committee[37] is a standing committee that reviews agency reports (refer to **Section 4.4** for information on agency reports), produces recommendations for revisions to this Policy, and advises the Chief Privacy Officer on timely privacy issues. Committee members serve renewable two-year terms.

The Identifying Information Law requires certain agencies to serve on the Citywide Privacy Protection Committee and allows the Mayor to designate additional agencies to serve.[38] The Chief Privacy Officer may nominate agencies to serve on the committee. Agency heads and commissioners with representation on the committee should designate representatives familiar with agency privacy policies and practices, aware of agency incident response and coordination efforts, and with knowledge of current legislative, regulatory, and policy developments relating to privacy protection.

[36] *See* Admin Code §§ 23-1202(c)(4) and (d)(1).
[37] The Citywide Privacy Protection Committee is the committee required by Admin. Code § 23-1204.
[38] *See* Admin. Code § 23-1204(a)(1).

5.0 Agency Collection, Use, Disclosure, Access to, and Retention of Identifying Information

5.1 Routine Collections and Disclosures of Identifying Information

Agency privacy officers must review all agency collections and disclosures of identifying information. They should designate collections and disclosures made in the agency's normal business operations as "routine." Agency privacy officers may designate collections or disclosures as "routine" at any time.

Collections or disclosures are "routine" if they meet a two-part test. First, they must be "made during the normal course of city agency business."[39] Second, they must "further the purpose or mission" of the agency.[40] Agency privacy officers must document their designations.

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

"Routine" collections or disclosures sometimes involve multiple agencies. Agencies may jointly approve these collections or disclosures if they further the purpose or mission of each agency.[41] Examples include agencies regularly exchanging identifying information with each other to administer a benefit program or service, to manage a mutually dependent ongoing interagency function like payroll operations, or to follow agency records retention policies.

Agency privacy officers are not required to make joint designations. Sometimes it may be burdensome to coordinate the documentation and reporting. Agency privacy officers may instead individually approve collections and disclosures as "routine."

5.1.1.1 Documenting Routine Pre-Approval by Agency Privacy Officers of Two or More Agencies

Where *multiple* agency privacy officers have pre-approved the same collection or disclosure as "routine," they may jointly document the pre-approval. The collecting agencies and disclosing agencies should have complementary and consistent descriptions in their reports. For example, when Agency A is disclosing the information to Agency B, then Agency A should report the *disclosure* as "routine" and Agency B should report the *collection* as "routine."

> ➢ **Guidance Tip:** In these circumstances, agency privacy officers should also develop a joint protocol to receive and investigate related complaints for violations of the Identifying Information Law. Refer to Section 8 for guidance on receiving and investigating complaints for violations of the Identifying Information Law.

[39] *See* Admin. Code § 23-1201.
[40] *Id.*
[41] *See id*.

5.1.2 Guidance for Making "Routine" Designations by Agency Function

Agency privacy officers may designate categories of collections and disclosures as "routine." These categories should match agency functions. Examples of agency functions are legal services, personnel administration, communications, constituent affairs, or information technology.

Agencies should still have internal protocols to ensure the appropriate level of internal review and approval for each routine collection or disclosure. A routine designation for an agency function does not mean that any and all identifying information should be collected or disclosed for that function without further internal agency review.

> ➢ **Guidance Tip:** For example, agency privacy officers can designate responding to subpoenas as routine, but each subpoena may contain data demands subject to specific laws or privileges. Agencies should have internal protocols requiring review of any laws, regulations, and privileges governing identifying information. Likewise, when agency privacy officers consider designating requests from oversight agencies as "routine," they should review each request to determine if any laws restrict the disclosure of identifying information, or if a confidentiality agreement is required.

5.1.2.1 Designating "Routine" Collections from or Disclosures to Third Parties

Some agency functions collect identifying information from or disclose it to third parties. Before designating those collections or disclosures as "routine," agency privacy officers should implement a protocol so that identifying information is collected or disclosed in accordance with this Policy and any applicable laws. Agencies may adopt the Model Protocols to meet this requirement. The protocol should be incorporated into the agency guidance referenced in **Section 1.5.5**.

5.1.3 Support in Making Agency Routine Designations

The authority to designate a collection or disclosure as routine rests with agency privacy officers. Agency privacy officers may consult the Chief Privacy Officer for advice on making routine designations. Agency privacy officers may ask the Chief Privacy Officer if the collection or disclosure can be approved as being in the best interests of the City. Refer to **Section 5.2.3** on how the Chief Privacy Officer makes best interests of the City determinations.

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

Agency privacy officers may approve collections and disclosures of identifying information that are not "routine" on a case-by-case basis. Collections and disclosures approved on a case-by-case basis must be required by law, made with the consent of the subject or their legal guardian, or further the purpose or mission of the agency.[42]

[42] *See* Admin. Code § 23-1202(b)(1) and (c)(1).

> ➢ **Guidance Tip:** Agency privacy officers should consider making case-by-case approvals where the collection or disclosure is a one-time activity not occurring during the normal course of agency business. Examples include a disclosure for a unique data-sharing initiative or a multi-agency study involving other agencies.

Agency privacy officers *may not* approve collections or disclosures of identifying information that are not "routine," not required by law, not consented to by an individual or their legal guardian, or that do not further the purpose or mission of the agency. These collections or disclosures should be denied or referred to the Chief Privacy Officer. The Chief Privacy Officer may approve *collections* of identifying information in the best interests of the City.[43] The Chief Privacy Officer may also approve *disclosures* of identifying information between City agencies in the best interests of the City.[44] Refer to **Section 5.2.3** on the Chief Privacy Officer's role in non-routine collections and disclosures.

> ➢ **Guidance Tip:** Some collections or disclosures can be approved by the Chief Privacy Officer and by agency privacy officers. Agency privacy officers should contact the Chief Privacy Officer for guidance on case-by-case requests for identifying information.

5.2.1 Determining Whether a Collection or Disclosure Is "Routine" or "Non-Routine"

Agency privacy officers may use "routine" and case-by-case pre-approvals as a way to manage their level of supervision over their agency's collections and disclosures of identifying information. Agency privacy officers should consider the following criteria when deciding if a collection or disclosure should be pre-approved as "routine" or considered on a case-by-case basis:

(i) Is the collection or disclosure frequent or does it involve recurring action by the agency?
(ii) Is the collection or disclosure made in the ordinary course of the agency's daily business?
(iii) Is the type of requesting entity involved with the normal business operations of the agency?

If the majority of answers are "no," consider approving the collection or disclosure on a case-by-case basis. Agency privacy officers should also consider other factors based on their agency's mission and purpose. "Routine" pre-approvals may be suitable for agency functions that need less agency privacy officer oversight (refer to **Section 5.1.2** for examples). Pre-approvals on a case-by-case basis may be appropriate for unique agency projects or circumstances or functions the agency privacy officer thinks need closer supervision.

[43] *See* Admin. Code §§ 23-1202(b)(2)(b).
[44] *See* Admin. Code §§ 23-1202(c)(2)(b).

- **Guidance Tip**: For example, an agency wants to report employee demographic information to senior City officials for an employment equity initiative. Since demographic information is identifying information, the agency privacy officer must approve the disclosure. Provided that no other law prohibits the disclosure, the agency privacy officer may:

(i) pre-approve it as "routine" as furthering the agency's purpose or mission *and* as a part of normal agency business, e.g., as part of the agency's EEO function. A "routine" designation means that the agency privacy officer does not need to approve future disclosures of identifying information for this function; or

(ii) approve it on a "case-by-case" basis as furthering the agency's purpose or mission *alone*, e.g., where the equity initiative requires a *single* disclosure (or set of disclosures) of identifying information because it is a unique project (such as a new study relating to the City's workforce). A "case-by-case" designation means that the agency privacy officer must approve any future disclosure of identifying information for this function; or

(iii) disapprove the disclosure upon finding that it does not further the agency's purpose or mission and refer the matter to the Chief Privacy Officer if appropriate.

5.2.1.1 Disclosures Not to be Treated as "Routine"

The Chief Privacy Officer may determine that certain disclosures of identifying information are not to be approved by agency privacy officers as routine.[45] Such disclosures require an additional level of review and approval by the agency privacy officer. Refer to **Section 4.3.4** for information on approvals of collections and disclosures on a case-by-case basis.

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

The Identifying Information Law does not interfere with agencies' obligations toward oversight authorities. When reviewing oversight requests for identifying information, agency privacy officers must authorize the disclosure, subject to **Section 5.2.2.1**, if:

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

(ii) the disclosing agency is not legally prohibited from disclosing the information to the oversight agency, and is not asserting a privilege; **and**

[45] *See* Admin. Code § 23-1203(5).

(iii) **one** of the following applies:

a. the agency privacy officer has pre-approved the disclosure of identifying information as "routine" (as either required by law or furthering the mission or purpose of the agency);[46] or

b. the agency privacy officer approves the disclosure, on a case-by-case basis, as required by law; or

c. 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 necessary confidentiality agreements and data security requirements;[47] or

d. the individual to whom the information pertains, or such individual's parent, legal guardian, or other person with legal authority to consent on behalf of the individual, has authorized in writing; or

e. the oversight agency is a City agency, and the Chief Privacy Officer pre-approves the collection and disclosure of the identifying information, respectively, by the oversight agency and the disclosing agency as in the best interests of the City.[48]

5.2.2.1 Requests Implicating Important Privacy Interests Including Sensitive Identifying Information

If an agency privacy officer approves the disclosure of identifying information to an oversight agency and the agency privacy officer or the Chief Privacy Officer determines that disclosure involves a risk of compromising an important privacy interest (e.g., the disclosure of sensitive identifying information), additional requirements are necessary. These include a confidentiality agreement and secure transmission and storage protocols that comply with the Citywide Information Management Standard and additional Citywide Cybersecurity Program Policies and Standards. Agencies should use a confidentiality agreement whenever possible, even if the disclosure of sensitive identifying information is required by law. Agency privacy officers should seek guidance from the Chief Privacy Officer if they have difficulty obtaining an agreement with an oversight agency.

[46] *See* Admin. Code 23-1202(c)(2)(a).
[47] *See* Admin. Code § 23-1202(c)(1)(b).
[48] *See* Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

- **Guidance Tip:** The use of confidentiality agreements for disclosing information from City agencies to City oversight agencies predates the Identifying Information Law. These agreements typically include commitments to safeguard information, report unauthorized disclosures to the source agency, and inform the source agency of third-party requests for information so it can take legal action. The Chief Privacy Officer or Office of Information Privacy can provide model agreements or help develop them.

- **Guidance Tip:** A confidentiality agreement with an oversight agency is appropriate if the requested identifying information may reveal the following: 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 confidential information about the City's cybersecurity or infrastructure assets; or individuals' medical information. Agency privacy officers may contact the Chief Privacy Officer for guidance on whether a confidentiality agreement is required.

- **Guidance Tip**: Referencing the Privacy Impact Assessment template in the **Agency Privacy Officer Toolkit** may help agencies think about whether disclosure of identifying information to an oversight agency involves a risk of compromising an important privacy interest.

5.2.2.2 Requests from the Department of Investigation

The Department of Investigation is the City's inspector general and has authority to investigate cases of fraud, corruption, and other illegal activities by City employees and contractors pursuant to its powers.[49]

Under the City Charter, the Department of Investigation is "authorized and empowered to make any study or investigation" that "may be in the best interests of the city,"[50] including "investigations of the affairs, functions, accounts, methods, personnel or efficiency of any agency."[51] When performing these duties, the Department has the authority to collect and review records, documents, and information (including identifying information) maintained or held by any agency.[52] The Identifying Information Law does not limit the Department's authority to perform its Charter-mandated law enforcement and oversight functions. Nothing in the Law or this Policy shall interfere with the Department of Investigation's ability to perform its duties in accordance with applicable law.[53] Disclosures of identifying information to the Department of Investigation pursuant to its powers are "required by law" within the meaning of the Identifying Information Law[54] and **Section 5.2.2.2**. Agency privacy officers should designate disclosures to the Department of Investigation as "routine" as described in **Section 4.3.3**, and agencies and agency privacy officers should fully cooperate with the Department of Investigation's requests.[55]

[49] *See* NYC Charter § 803 and Executive Order No. 16 of 1978.
[50] NYC Charter § 803(b).
[51] *Id.*
[52] *See* Executive Order No. 16 of 1978 § 4(a).
[53] *See* Admin. Code §23-1202(i).
[54] *See* Admin. Code §23-1202(c)(1)(c).
[55] *See* NYC Charter § 1128.

> ➢ **Guidance Tip:** Due to the nature of the Department of Investigation's work, agencies should work collaboratively with DOI. If an agency privacy officer has a privacy-related question about a Department of Investigation request, they should, together with the Department of Investigation, consult the Chief Privacy Officer within a reasonable amount of time after receiving the request. The agency privacy officer, the Department of Investigation, and the Chief Privacy Officer will collaborate to resolve any concerns raised by the agency.

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

The Chief Privacy Officer may approve two kinds of non-routine collections or disclosures. First, the Chief Privacy Officer can approve collections of identifying information if they are in the best interests of the City.[56] Second, the Chief Privacy Officer can approve disclosures to City agencies upon determination that such disclosure is in the best interests of the City.[57]

For example, an agency privacy officer may not approve a disclosure as part of a multi-agency data-sharing project unless the project furthers the purpose or mission of the disclosing agency. But the Chief Privacy Officer can approve the disclosure if this initiative serves a broader City purpose of enhancing the health, welfare, or safety of New Yorkers.

These determinations are made sparingly. 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, before referring potential collections or disclosures of identifying information to the Chief Privacy Officer for best interests of the City determinations.

When referring a proposed collection or disclosure of identifying information to the Chief Privacy Officer for a best interests of the City determination, agency privacy officers should provide information necessary for the Chief Privacy Officer to assess the circumstances that the agency privacy officer believes warrants the determination. The Chief Privacy Officer will review the referral, may engage with the agency privacy officer to understand and narrow the referral, and may issue a written determination approving the collection or disclosure.

> ➢ **Guidance Tip:** Refer to the **Agency Privacy Officer Toolkit** for the Best Interests of the City Worksheet and instructions for referring a proposed collection or disclosure to the Chief Privacy Officer.

5.3 Collections and Disclosures Involving Investigations

Agency privacy officers do not need to approve collections by or disclosures 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.[58]

[56] *See* Admin. Code § 23-1202(b)(2)(b).
[57] *See* Admin. Code § 23-1202(c)(2)(b).
[58] *See* Admin. Code §§ 23-1202(b)(2)(c)(1) and (c)(2)(c)(1).

Agency privacy officers do not need to approve collections by or disclosures to a City agency in connection with an open investigation concerning the welfare of a minor or an individual who is otherwise not legally competent.[59]

5.4 Collections and Disclosures Made Under Exigent Circumstances

Agencies may collect or disclose identifying information under exigent circumstances (refer to **Section 3.2.10** for the definition of exigent circumstances). The authority to collect or disclose identifying information under exigent circumstances is limited to the time necessary to resolve the urgency. Exigent circumstances are not a blanket exception to agency privacy officer or Chief Privacy Officer review and approval.

> ➢ **Guidance Tip:** For example, disclosing identifying information about known occupants of a location following an unforeseen event like 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 public health and safety. It would be impracticable for an agency privacy officer to conduct a typical review before disclosing identifying information (e.g., 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 is not possible, disclosing individuals' contact information without prior approval from the agency privacy officer to an alternate City vendor to deliver emergency food would be permissible under exigent circumstances.

5.4.1 Reporting Collections and Disclosures Made Under Exigent Circumstances

Agency privacy officers must report collections or disclosures made under exigent circumstances, along with an explanation of why exigent circumstances existed, to the Chief Privacy Officer. Agency privacy officers must notify the Chief Privacy Officer within 24 hours of becoming aware of the collection or disclosure, except where such notification is expressly exempted under Admin. Code § 23-1202(d)(1), even if they do not have complete information. 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

Agencies should refer to the Model Protocols when responding to requests and proposals for the collection or disclosure of identifying information (refer to **Section 1.5.5** for information on the Model Protocols). Proposals for identifying information may need on-going disclosures, which require more agency resources. For example, a proposal may involve weekly transmission of updated files or use technologies the agency does not have. Agency privacy officers should work with their counsels and programmatic and technical staff to determine the legality and feasibility of the proposals. Agencies may also consider completing or referencing the Privacy Impact Assessment, located in the **Agency Privacy Officer Toolkit**, to better evaluate the privacy risks of a given request or proposal.

Agency privacy officers should carefully evaluate requests or proposals involving sensitive identifying information, which requires contractual terms governing its disclosure (refer to **Sections 6.1.3**, **6.2.1** and "Guidance for Drafting Contract Terms to Protect Sensitive Identifying Information" in the **Agency Privacy Officer Toolkit** details).

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

Agencies that maintain repositories of identifying information should develop policies for considering and responding to requests and proposals for the collection and disclosure of identifying information. The policies should consider the laws that apply to the repositories, the kinds of identifying information likely to be requested, and the anticipated uses of disclosed identifying information.

> ➢ **Guidance Tip:** Agency privacy officers should consult with the Chief Privacy Officer and the 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 agreements.

5.5.1 Privacy Impact Assessments

A privacy impact assessment can assist agency privacy officers in analyzing and integrating privacy considerations into the information handling and risk management aspects of their agencies' operations. Agency privacy officers are encouraged to conduct a privacy impact assessment before their agencies implement projects that change how the agency collects, uses, or discloses identifying information. Once conducted, agency privacy officers should periodically reassess and prepare a revised privacy impact assessment if there are substantive changes to how a project will collect, use, or disclose identifying information.

> ➢ **Guidance Tip:** Refer to the **Agency Privacy Officer Toolkit** for the Privacy Impact Assessment template.

5.6 Privacy-Enhancing Techniques and Technologies

Privacy-enhancing techniques and technologies are tools or methods to increase the privacy of identifying information when it is collected, used, disclosed, or retained. Agency uses of privacy-enhancing techniques and technologies implement the Privacy Principle of Data Minimization. Agencies must consider whether and which privacy-enhancing techniques and technologies are appropriate (refer to **Section 5.6** for related guidance on privacy by design). Agencies should encourage employees to consult with agency privacy officers for support when determining how to minimize the collection and disclosure of identifying information. Agencies should also work with their covered contractors and subcontractors to minimize the collection or disclosure of identifying information.

To determine the appropriate privacy-enhancing techniques and technologies for a project, agency privacy officers should analyze the contextual integrity (refer to **Section 3.2.8**) of the identifying information to be processed, consider the Privacy Principles, and evaluate the costs, risks, and benefits of implementing the applicable privacy-enhancing techniques and technologies. Refer to Guidance on Implementing Privacy by Design in the **Agency Privacy Officer Toolkit** for additional information regarding this process. Agency privacy officers should collaborate with technology professionals, attorneys, and business staff to carefully evaluate the use of privacy-enhancing techniques and technologies.

Many privacy-enhancing techniques and technologies are in an early stage of development. Agency privacy officers should collaborate with technical colleagues, attorneys, and business staff to carefully evaluate how they will affect the agency's operations, the level of technical expertise required, and the expected privacy enhancement.

- **Guidance Tip:** Contact Cyber Command for security guidance on privacy-enhancing techniques and technologies.
- **Guidance Tip**: Completing the Privacy Impact Assessment template in the **Agency Privacy Officer Toolkit** may help agency privacy officers determine the appropriate privacy-enhancing techniques and technologies for a given project.

5.6.1 Chief Privacy Officer Role in Privacy-Enhancing Techniques and Technologies

The Chief Privacy Officer may require an agency to use anonymization methods or privacy-enhancing techniques and technologies where appropriate to minimize the collection or disclosure of identifying information, in accordance with the agency's mission or purpose.[60]

5.7 Retention of Identifying Information

The Identifying Information Law does not interfere with any law or policy that requires agencies to keep identifying information.[61] Agencies should keep identifying information contained in their records for as long as required by their Records Retention and Disposition Schedules or any other laws or policies that apply to them.

Agencies may not dispose of records that are subject to a retention schedule without the approval of the Commissioner of the Department of Records and Information Services, the Corporation Counsel for the City of New York, and the agency head that has jurisdiction over the records.

Agencies may keep identifying information to further their missions or purposes. They may also keep identifying information if retention is in the best interest of the City and is not contrary to their missions or purposes. Agency privacy officers should consult with their counsels and records management officers to decide whether keeping identifying information furthers their agency's mission or purpose.

Agency privacy officers should coordinate with their agency records officers to make sure that staff know their retention policies. In all cases, agencies should limit access to identifying information to authorized users who have a business need for access and to the staff responsible for storage and maintenance of the information.

5.7.1 Data Storage and Maintenance Requirements

Agencies must follow City policy when storing identifying information, including the Citywide Information Management Standard, Citywide Cybersecurity Program Policies and Standards, and this Policy.

5.7.2 Disposal of Identifying Information

Agencies must minimize the risk of unauthorized or inadvertent disclosure when disposing of identifying information. Agencies must properly dispose of electronic equipment and records containing identifying information, including by following the **Citywide Cybersecurity Requirement for the Reuse and Disposal of Systems and Non-Computing Storage Devices Policy** and **Citywide Cybersecurity Requirement for the Re-use**

[60] Admin. Code § 23-1203(1).
[61] Admin. Code § 23-1202(e).

and Disposal of Systems and Non-Computing Storage Devices Standard.[62] Agency privacy officers should work with records access officers to identify disposal requirements and to dispose of identifying information as provided by their Records Retention and Disposition Schedules approved by the Department of Records and Information Services.

Agency personnel should immediately notify their agency privacy officer if they discover that identifying information was disposed of improperly.

5.8 Program-Specific Privacy Policies

When interacting with individuals through digital products such as websites or apps, or through traditional programs, agencies should use program-specific privacy policies to clearly describe how identifying information is collected, used, shared, and stored. Agency privacy officers, in collaboration with agency counsel and other stakeholders, should draft, review, and update program-specific privacy policies at regular intervals to ensure they remain accurate and reflect any changes in data practices, business operations, and legal requirements.

Program-specific privacy policies should be tailored to the programs to which they apply. Generally, program-specific privacy policies should discuss the purpose of the program and policy, the agency to which it applies, the types of identifying information collected and for what purpose they are collected, how long the identifying information is retained, and how and with whom identifying information will be disclosed.

Program-specific privacy policies should also clearly define the terms they use, what options individuals have with respect to the identifying information covered by the policies, how the agency protects the identifying information it collects, and what technologies are used to collect identifying information.

Program-specific privacy policies must identify the effective date of the policy, how updates to the policy will be communicated to individuals, and include a method for individuals to contact the agency privacy officer.

Creating an effective privacy policy requires collaboration across the agency to ensure both legal compliance and practical applicability. Collaboration between agency divisions is crucial to ensure that every aspect of data collection, usage, and protection is captured with precision. By engaging relevant stakeholders, the privacy policy should become a true representation of the agency's actual practices. Key stakeholders may include legal and compliance; IT and security; program management or product and development; communications and customer service; risk management; and senior leadership.

6.0 Contracts

6.1 Contracts Subject to the Identifying Information Law (Covered Contracts)

Covered contracts must include the Identifying Information Rider. The Identifying Information Rider is a standard document related to the protection of identifying information.[63] The Identifying Information 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.

[62] *See* Admin. Code §§ 10-503 and 10-504.
[63] *See* Admin. Code § 23-1203(7).

The Identifying Information Rider was revised with version 4.0 of this Policy. The revision is effective **April 1, 2025**.

Agencies may attach both the Identifying Information Rider and the Privacy Protection Rider to the same contract. Refer to the **Agency Privacy Officer Toolkit** for the Identifying Information Rider and Privacy Protection Rider.

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.[64] 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.[65]

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 are subject to the requirements of the Identifying Information Law, **effective for any 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 (refer to **Section 3.2.11** for the definition of "sensitive identifying information"); 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**.

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 where "technology" (as defined by the **State Technology Law**) 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, or which make sensitive identifying information accessible to the contractor or subcontractor in connection with such contract or subcontract, even if the access is not the express purpose of the contract. Refer to **Section 3.2.11** for guidance on sensitive identifying information.

This definition also includes 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.

This definition excludes (i) contracts where the vendor simply provides a technology product to the City, like basic computer hardware or on-premise software not involving the vendor's access to sensitive identifying information; and (ii) subcontracts for technology services that generally govern a contractor's business relationships as a whole (i.e., for a broad range of clients, not just the City alone), provided that the City contractor includes appropriately protective privacy and security provisions in such subcontracts.

[64] *See* Admin. Code § 23-1201.
[65] *See* Admin. Code §§ 23-1201 and 6-129(c)(21).

- **Guidance Tip:** Examples of such contracts include those where (i) 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) 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.

- **Guidance Tip:** Contractors and subcontractors are also required to follow the Citywide Cybersecurity Program Policies and Standards for handling, storing, encrypting, labeling, and transmitting sensitive identifying information. Refer to **Section 1.5.3** for information on the Citywide Cybersecurity Program Policies and Standards.

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, discloses, or accesses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies, offices, or members of the public access information about City services, resources, or events. The agency that is the source of the identifying information should identify such contracts and subcontracts in consultation with its agency privacy officer and the Chief Privacy Officer.

"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, but are not limited to, in-person or telephone contact, text-messaging, email, mail, or website postings.

This designation of certain outreach contracts only applies to projects led by a City agency or office that engages a vendor for outreach on behalf of other City agencies' clients, but does not include agency contracts with a vendor for outreach to the agency's own clients. Agencies using vendors for outreach to their own clients through contracts or subcontracts not covered under this Policy should attach the Privacy Protection Rider to these contracts or subcontracts.

- **Guidance Tip:** Examples of such contracts 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 provide information about emergency services to the clients of City agencies, offices, or members of the public, where a contractor or subcontractor will collect the identifying information from an entity other than the lead agency or office for purposes such as: emailing, texting, or mailing information about available City services; notification of an upcoming town hall; or providing information about eligibility for a public benefit program.

6.1.3 Modifications to the Identifying Information Rider

The Chief Privacy Officer has designated the Identifying Information Rider as a standard contract provision.[66] Agencies must use the standard text of the Identifying Information Rider. If an agency believes that exceptional circumstances warrant modifying part of the Identifying Information Rider, it may submit a written request to the Chief Privacy Officer seeking approval to deviate from the standard text.

When requesting a deviation, agency privacy officers should provide information necessary for the Chief Privacy Officer to assess the exceptional circumstances that the agency privacy officer believes warrant a deviation, justifications for each requested deviation, and an explanation for the agency's proposed compensating privacy controls. The Chief Privacy Officer will review the request, may engage with the agency and the contractor to understand and narrow the request, and will issue a written determination approving or denying the request for a deviation.

Agencies should advise potential contractors early in the contracting process that the standard text of the Identifying Information Rider is mandatory. This will allow sufficient time for the agency and contractor to understand whether a deviation request is necessary, prepare and submit the request, have it fully considered, and for the Chief Privacy Officer to issue a determination.

- **Guidance Tip:** Refer to the **Agency Privacy Officer Toolkit** for instructions on submitting a request for a deviation.
- **Guidance Tip:** Deviations from the Identifying Information Rider may affect other aspects of a contract. Agencies should consult the Law Department for guidance on all aspects of pending contracts, as appropriate.

6.1.4 Non-Covered Contracts Involving the Collection, Use, Disclosure, and Access to Sensitive Identifying Information

When a contract or subcontract of any value involves the collection, use, disclosure, or access to sensitive identifying information, but is not a covered contract, agencies must include provisions in those contracts to appropriately protect the privacy and security of the sensitive identifying information. Agencies may adapt the Privacy Protection Rider for this purpose. Agencies may also draft their own privacy protection terms. Refer to the **Agency Privacy Officer Toolkit** for the Privacy Protection Rider and guidance for drafting privacy protection terms.

- **Guidance Tip**: Completing or referencing the Privacy Impact Assessment template in the **Agency Privacy Officer Toolkit** may help agencies draft privacy protection terms that appropriately protect sensitive identifying information.

[66] *See* Admin Code 23-1203(7).

6.2 Requirements for Data Sharing Agreements

6.2.1 When an Agreement Is Required

Agencies should have data sharing agreements before disclosing identifying information as a best practice. However, data sharing agreements are generally not needed for each "routine" disclosure or if the agency privacy officer determines that there is not a risk that an important privacy interest will be compromised. Agency privacy officers may consult with the Chief Privacy Officer and their agency's Chief Contracting Officer to decide whether there is a risk to an important privacy interest.

Sometimes even "routine" disclosures need data sharing agreements. Agencies should consider the nature or extent of the disclosure and the relationship of the agency to the third party.

Agency staff should consult with their agency privacy officer to identify when an agreement is needed. Such disclosures include:

- identifying information that is restricted by other laws or regulations;
- transferring custody and maintenance of identifying information to a third party; or
- sensitive identifying information;
- where an agreement is already needed for other reasons, such as insurance or intellectual property ownership.

When a law, regulation, or oversight agency requires a particular format for a data sharing agreement, agencies should use that form. When no particular form is needed, agencies should refer to the **Agency Privacy Officer Toolkit** for template agreements. Agencies may also develop their own forms and may consult with the Chief Privacy Officer for assistance in developing forms tailored to their needs.

> ➢ **Guidance Tip:** Refer to **Section 5.2.2** for responding to requests for identifying information from oversight agencies and drafting agreements when requests involve disclosure of sensitive identifying information.
>
> ➢ **Guidance Tip:** Refer to the **Agency Privacy Officer ToolkitAgency Privacy Officer ToolkitU** for guidance on drafting agreements that involve disclosure of sensitive identifying information.

6.2.2 Elements of Data Sharing Agreements

Each data sharing agreement involving identifying information should be tailored to the unique facts and circumstances of the data sharing, including 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 agreements involving identifying information:

- A scope of work that includes the purpose for using the information, the specific 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 disclosed, and by whom, along with any legal basis for the disclosure.
- Restrictions on access to the information to authorized users for a permitted purpose.
- Limits on further disclosure to third parties without prior written authorization, or unless by law, subpoena, or court order.
- Requirement of reasonable physical, technical, and procedural safeguards to protect the security of the information.
- Requirement to cooperate with City investigations into unauthorized disclosures.

> ➢ **Guidance Tip:** Sample privacy protection language is provided in the **Agency Privacy Officer Toolkit**. Agency privacy officers or agency counsel may seek further guidance from the Chief Privacy Officer in developing agreements for sharing identifying information.

6.2.3 Review by the Law Department

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

7.0 Training and Education Requirements

7.1 Citywide Privacy Training

The Chief Privacy Officer has developed citywide privacy protection training for agency employees and covered contractors and subcontractors. The training covers the general requirements of the Identifying Information Law and how agency employees and contractors should handle identifying information. Agency privacy officers may access and deploy the training, which is available at the Department of Citywide Administrative Services' **Citywide Training Center**, to all their employees or to specific groups of employees at their agencies.

7.2 Supplemental Agency Training

Agency privacy officers may develop privacy training suitable for their covered contractors' and subcontractors' unique practices and needs. This training must be consistent with the citywide privacy training implemented by the Chief Privacy Officer, and any laws or policies regarding the collection, retention, and disclosure of identifying or other confidential information. For example, if the agency collects, retains, and discloses tax information, supplemental training should cover how to protect tax information. Agency privacy officers should consult with their counsel and the Chief Privacy Officer in developing supplemental training.

> ➢ **Guidance Tip:** The **Agency Privacy Officer Toolkit** contains training slides that can be incorporated into supplemental agency training.

7.3 Agency Implementation of Training Requirements

Agency privacy officers should identify personnel, as well as contractors and subcontractors, who should receive privacy training. They should consider typical job functions and the level of access to identifying information they require. Agency privacy officers should periodically train designated personnel and covered contractors and subcontractors so they remain current with privacy and confidentiality requirements relevant to their job functions.

7.4 Cybersecurity Awareness Training

Cyber Command offers cybersecurity awareness training that is intended to help employees remain aware of potential threats that could result in an incident or compromise the availability or integrity of identifying information to which an employee may have access. Agency privacy officers should coordinate their trainings with their chief information security officers to support privacy and cybersecurity.

8.0 Protocol for Receiving and Investigating Complaints

The Chief Privacy Officer accepts and investigates complaints (refer to **Section 3.2.6** for the definition of "complaint") related to of the Identifying Information Law.[67] Agency privacy officers must work with the Chief Privacy Officer to follow this requirement, as described in **Sections 8.2** and **8.3**.

8.1 Violations

Agency employees, contractors, and subcontractors are prohibited from collecting or disclosing identifying information except as provided in the Identifying Information Law. The Chief Privacy Officer may deem agencies as violating the Identifying Information Law if they do not comply with the Identifying Information Law or this Policy. Violations will be reported by the Chief Privacy Officer according to Admin. Code § 23-1202(c)(4) and **Section 4.4.2**.

8.1.1 Reporting Contractor Violations

If an agency's contractor or subcontractor discloses identifying information in violation of the Identifying Information Law, the agency must report the violation to the Chief Privacy Officer. This applies both to covered contracts (refer to **Section 6.1.1** and **6.1.2**) and to non-covered contracts involving identifying information.

> ➢ **Guidance Tip:** The Chief Privacy Officer reviews each agency report of a violation of the Identifying Information Law. The Chief Privacy Officer may contact the reporting agency privacy officer to learn more about the facts underlying the report to determine whether further action is necessary and to collaborate on measures to reduce or prevent similar subsequent violations.

8.2 Receiving Complaints

Agencies must adopt a written protocol for receiving and investigating complaints under the Identifying Information Law. Agencies are encouraged to publish the protocols on their public-facing websites. The protocol must, at a minimum:

[67] *See* Admin. Code § 23-1203(9).

- Designate a role-based mailbox, or equivalent, for receiving such complaints.
- Designate the agency privacy officer as the point of contact for receiving and investigating such complaints.
- Describe how to make complaints.
- Require the agency privacy officer to promptly investigate the complaint.
- Require the agency privacy officer to work with internal legal, program, technical, or other staff, including the Chief Information Security Officer, to investigate.
- Require the agency privacy officer to assess the impact of any applicable laws or policies.
- Require the agency privacy officer to notify the Chief Privacy Officer of the complaint within 24 hours of discovery;[68] and
- Provide for other City offices to be engaged, including the Chief Privacy Officer, the Law Department, Cyber Command[69], and others that can help investigate the complaint and advise on a response.

Agencies must create a form for receiving complaints. The form should collect information necessary for the agency privacy officer to commence an investigation, such as the complainant's contact information, the date the complainant became aware of the circumstances, a description of the circumstances, and any supporting documentation the complainant wishes to provide. Refer to the Agency Privacy Officer Toolkit for a sample complaint form.

Agencies must make the form available for online submission via their public-facing websites. Agencies may also allow complaints to be received via other methods. The form must be available to agency personnel, covered contractors and subcontractors, and the public.

> ➢ **Guidance Tip:** Because receiving a complaint is a collection of identifying information, agencies should consider designating it as a routine collection of identifying information. Refer to **Section 4.3.3** for information on routine designations.

8.2.1 Notification of Received Complaints

Agency privacy officers must notify the Chief Privacy Officer within 24 hours if they know or suspect that identifying information has been improperly used, disclosed, or accessed. Such notification must be made using a form or method prescribed by the Chief Privacy Officer unless the circumstances make it impossible, impractical, or imprudent to do so, or when using the prescribed notification form or method unreasonably delays notification. In exceptional cases where an agency privacy officer uses a non-prescribed notification method, the agency privacy officer must follow up that notification with the prescribed notification method. Following notification, the Chief Privacy Officer will engage agency privacy officers for purposes of keeping abreast of any new facts, helping engage appropriate stakeholders such as the Law Department or Cyber Command for further investigation and response, and advising on legal strategy or obligations such as breach notifications and credit monitoring.

[68] *See* Admin. Code § 23-1202(c)(4).

[68] Not all complaints that may impact privacy are cybersecurity matters. For suspected cybersecurity matters, contact Cyber Command at by email at [redacted] or [redacted], or by phone at [redacted].

> ➢ **Guidance Tip**: Agencies may be subject to additional notification requirements beyond those outlined in the Law and this Policy. Agency privacy officers should review any additional regulatory and contractual reporting obligations that may apply.

8.3 Investigating Complaints

Agencies must have in place a plan for investigating complaints relating to the Identifying Information Law. Upon receipt of a complaint, whether from internal or external sources, the agency privacy officer must initiate an investigation. The **Agency Privacy Officer Toolkit** provides guidance on how to investigate a complaint and agency privacy officers are encouraged to adapt this guidance to the unique requirements of their agencies. The guidance is focused on cyber-related incidents as cybersecurity is increasingly important, but the concepts of prudent communication, comprehensive fact-gathering, remediation, and legal assessment are applicable to all investigations.

Agencies should be aware that a potential violation of the Identifying Information Law may implicate other City entities as well. Guidance included in the **Agency Privacy Officer Toolkit** emphasizes the importance of a collaborative and coordinated approach that can leverage the City's investigatory resources and expertise most efficiently.

Agencies should contact the Chief Privacy Officer as necessary for additional guidance.

8.4 Notification Requirements

Agencies must make reasonable efforts to notify individuals in writing as soon as practicable when their identifying information has been used, disclosed, or accessed in violation of the Identifying Information Law when:

(i) Required by law or regulation;
(ii) There is potential risk of harm to the individuals, including a risk of harm that may be physical, financial, reputational, or other harm dependent upon any protected status of an individual, status as a victim or witness to a crime, or similar considerations; or
(iii) Where the agency privacy officer determines, in consultation with the Chief Privacy Officer, that notifying the individuals is prudent.

8.4.1 Additional Actions Pertaining to Notification

Other actions may also be appropriate. For example, credit monitoring may be advisable where a Social Security number or bank account information has been disclosed. If a domestic violence survivor's home address has been improperly released, recommending a change of door locks 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 other actions. Solutions beyond minimum no-cost credit and identity monitoring should be considered. The Model Investigation Plan contains guidance on assessing whether and how to offer other solutions.

Agencies and covered contractors and subcontractors should consider the following minimum standards when issuing notifications and offering identity protection services:

- Identity protection services offered at no cost to any affected individual.
- Identity protection services coverage for at least 24 months.
- Notifications associated with identity protection services clearly state the information necessary to take advantage of the offer, including how to enroll in the services.
- Identity protection services include credit monitoring, identity monitoring, and identity restoration services.
- Identity protection services include identity theft insurance of at least $1,000,000 in coverage to each affected individual.
- The total cost of identity protection services of at least $10 per year per enrollee.
- Identity protection services meet a commercially reasonable standard.

> ➢ **Guidance Tip:** Agencies should consult the Chief Privacy Officer if they believe that exceptional circumstances warrant deviating from the minimum standards.

The **Agency Privacy Officer Toolkit** provides additional information on notification requirements as well as sample notification language and instructions for accessing the citywide credit monitoring contract. This guidance is not intended to be comprehensive, and agency privacy officers remain responsible for ensuring compliance with requirements applicable to their agencies and circumstances.

Agencies or contractors may, in some cases, seek to provide notifications and identity protection services independently of the citywide credit monitoring contract. In such cases, agencies and contractors must obtain approval from the Chief Privacy Officer before engaging vendors outside the citywide credit monitoring contract.

Page Intentionally Blank

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

As of 2018, 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

Appendix B – 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 an agency.	3.2.3 Anonymization 5.6 Privacy-Enhancing Techniques and Technologies
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.	5.2.2.2 Requests from the Department of Investigation 5.2.2 Guidance for Responding to Requests for Identifying Information from Oversight Agencies 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 5.2.2.2 Requests from the Department of Investigation 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 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 Administrative Code 10-501 – 10-504 (Agency Disclosures of Security Breaches) 8.4 Notification Requirements Agency Privacy Officer Toolkit (Identifying Information Rider) Agency Privacy Officer Toolkit (Privacy Protection Rider) Agency Privacy Officer Toolkit (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 6.1.4 Non-Covered Contracts involving the Collection, Use, and Disclosure of Sensitive Identifying Information 6.2.2 Elements of Data Sharing Agreements Agency Privacy Officer Toolkit (Identifying Information Rider, Privacy Protection Rider, 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 Complaints 8.3 Investigating Complaints