



MICHAEL FITZPATRICK
CHIEF PRIVACY OFFICER

Citywide Privacy Protection Policies and Protocols

February 6, 2023

Version 3.0

Page Intentionally Blank

VERSION CONTROL

Version	Description of Change	Approver	Date
3.0	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Hyperlinked to all external documents where mentioned. Hyperlinked to sections of the Policy where referenced.</p>	<p>Michael Fitzpatrick</p> <p>Chief Privacy Officer, City of New York</p>	2/6/2023
2.1	<p>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.</p> <p>Updated the Chief Privacy Officer’s name to reflect current appointee.</p> <p>Updated hyperlinks to reflect website revisions.</p>	<p>Michael Fitzpatrick</p> <p>Chief Privacy Officer, City of New York</p>	10/6/2022
2.0	<p>Introduced guidance tips, made clarifications, and added sub-sections.</p> <p>Expanded NYS Freedom of Information Law and NYC Open Data Law guidance.</p> <p>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.</p> <p>Enhanced guidance relating to requests from oversight agencies.</p> <p>Designated technology services involving sensitive identifying information and certain outreach contracts and subcontracts as subject to the Identifying Information Law.</p> <p>Enhanced guidance relating to contracts and “routine” designations.</p>	<p>Laura Negrón</p> <p>Chief Privacy Officer, City of New York</p>	2/24/2021

	<p>Introduced recommendation for agencies to publish their privacy protocols to agency websites.</p> <p>Updated and added appendices, including new Privacy Protection Rider.</p>		
1.0	First Version	<p>Laura Negrón Chief Privacy Officer, City of New York</p>	1/28/2019

Page Intentionally Blank

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

Table of Contents

1.0	Introduction.....	1
1.1	Purpose and Scope.....	1
1.2	Authority	1
1.3	Applicability.....	1
1.4	Modification.....	1
1.5	Relationship to Other City and Agency Policies	2
1.5.1	Executive Order No. 3 of 2022.....	2
1.5.2	Agency Privacy Policies, Protocols, and Practices.....	2
1.5.3	Citywide Information Technology and Security Policies and Standards	2
1.5.3.1	Agency Privacy Officer Role in Ensuring Compliance with Citywide Information Technology and Security Policies and Standards	3
1.5.4	Mayoral Directive 2015-3: Uniform Records Management Practices.....	3
1.5.5	Model Protocols for Handling Third Party Requests for Information Held by City Agencies	3
1.5.6	General Confidentiality Policy.....	3
1.6	Relationship of the Identifying Information Law to Other Laws.....	4
1.6.1	New York State Freedom of Information Law	4
1.6.1.1	Publishing FOIL Request Titles on the Open Records Portal	4
1.6.2	Open Data Law.....	5
1.6.3	Administrative Code 10-501 – 10-504 (Agency Disclosures of Security Breaches)	5
2.0	Privacy Principles	5
3.0	Definitions and Key Terms	7
3.1	Definition of Identifying Information.....	7
3.1.1	Additional Types of Identifying Information Designated by the Chief Privacy Officer.....	8
3.1.2	Guidance in Determining When Other Information Constitutes Identifying Information	8
3.2	Clarification of Terms Not Defined in the Identifying Information Law	8
3.2.1	Access.....	8
3.2.2	Anonymized	8
3.2.3	Collection	9

3.2.4	Complaint.....	9
3.2.5	Disclosure.....	9
3.2.6	Exigent Circumstances	9
3.2.7	Sensitive Identifying Information	9
3.2.7.1	Requirements When Handling Sensitive Identifying Information	9
3.2.8	“Requests” for Identifying Information	10
3.2.9	“Proposals” for Identifying Information	10
3.2.10	Use	10
4.0	Agency Privacy Officer.....	10
4.1	Designation	10
4.1.1	Agency Employee Designations	10
4.1.1.1	Records Access Officer.....	10
4.1.2	Contractors and Subcontractors.....	11
4.1.3	Agency Privacy Officer Training	11
4.2	Agency Privacy Officer Responsibilities	11
4.2.1	Agency Privacy Protection Policies and Guidance	11
4.2.2	Agency Compliance Plan.....	11
4.2.3	Agency Liaison Network.....	11
4.2.3.1	Descriptions of Key Agency Executive Roles.....	11
4.2.4	Agency Privacy Officer Toolkit	12
4.3	Approval of Collections and Disclosures	12
4.3.1	Pre-approval as Routine.....	13
4.3.2	Approval on a Case-by-Case Basis of Collections and Disclosures That Are Not “Routine”	13
4.3.3	Exemptions for Collections or Disclosures.....	13
4.3.3.1	Exemption for Collections or Disclosures Involving Police Investigations.....	13
4.3.3.2	Exemption for Collections or Disclosures Involving Child Welfare Investigations	13
4.4	Reporting.....	14
4.4.1	Agency Reports	14
4.4.2	Quarterly Report on Unauthorized Disclosures and Collections or Disclosures Made Under Exigent Circumstances	14
4.4.2.1	Timing of Reporting Unauthorized Disclosures and Collections or Disclosures Made Under Exigent Circumstances	14
5.0	Agency Collection, Use, Disclosure, Access to, and Retention of Identifying Information	15
5.1	Routine Collections and Disclosures of Identifying Information	15
5.1.1	Pre-approval as Routine by Agency Privacy Officers of Two or More Agencies.....	15
5.1.1.1	Documenting Routine Pre-Approval by Agency Privacy Officers of Two or More Agencies.....	15

5.1.2	Guidance for Making “Routine” Designations by Agency Function	15
5.1.2.1	Designating “Routine” Collections from or Disclosures to Third Parties.....	16
5.1.3	Support in Making Agency Routine Designations.....	16
5.2	Agency Privacy Officer Approval of Collections and Disclosures of Identifying Information on a Case-by-Case Basis	16
5.2.1	Determining Whether a Collection or Disclosure is “Routine” or “Non-Routine”	17
5.2.2	Guidance for Responding to Requests for Identifying Information from Oversight Agencies.....	17
5.2.2.1	Requests Implicating Important Privacy Interests Including Sensitive Identifying Information ...	18
5.2.3	Chief Privacy Officer Role in Non-Routine Collections and Disclosures	19
5.3	Collections and Disclosures Involving Investigations.....	19
5.4	Collections and Disclosures Made Under Exigent Circumstances	19
5.4.1	Reporting Collections and Disclosures Made Under Exigent Circumstances	20
5.5	Requests and Proposals for Identifying Information	20
5.6	Data Minimization.....	20
5.6.1	Anonymization	20
5.7	Retention of Identifying Information.....	21
5.7.1	Data Storage and Maintenance Requirements	21
5.7.2	Disposal of Identifying Information	21
6.0	Contracts.....	22
6.1	Contracts Subject to the Identifying Information Law (Covered Contracts)	22
6.1.1	Contractors and Subcontractors Subject to the Identifying Information Law	22
6.1.2	Contracts and Subcontracts for Other Services Designated by the Chief Privacy Officer	22
6.1.2.1	Contracts and Subcontracts for Technology Services Involving Sensitive Identifying Information	23
6.1.2.2	Contracts and Subcontracts for Outreach Services Involving Identifying Information	23
6.1.3	Non-Covered Contracts Involving the Collection, Use, Disclosure, and Access to Sensitive Identifying Information.....	24
6.2	Requirements for Data Sharing Agreements	24
6.2.1	When an Agreement is Required.....	24
6.2.2	Elements of Data Sharing Agreements	25
6.2.3	Review by the Law Department.....	25
7.0	Training and Education Requirements.....	25
7.1	Citywide Privacy Training	25
7.2	Supplemental Agency Training	25
7.3	Agency Implementation of Training Requirements.....	26
7.4	Cybersecurity Awareness Training.....	26

8.0 Protocol for Receiving and Investigating Complaints for Violations of the Identifying Information Law ... 26

- 8.1 Violations 26
- 8.2 Receiving Complaints 26
 - 8.2.1 Notification of Received Complaints 27
- 8.3 Investigating Complaints..... 27
- 8.4 Notification Requirements..... 27
 - 8.4.1 Additional Actions Pertaining to Notification 27

Appendix A – List of City Entities Exempt from the Identifying Information Law..... 29

Appendix B – Table Cross-Referencing CPO Policy with Required Provisions under Section 23-1203 of the Administrative Code 31

Page Intentionally Blank

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 Information Technology and Security 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 Information Classification Policy (P-ID-RA-01)
- Citywide Information Classification Standard (S-ID-RA-01)
- Citywide Information Management Policy (P-01-PR-DS)
- Citywide Information Management Standard (S-01-PR-DS)
- Citywide Cybersecurity Categorization of Data and System Policy (P-03-ID-RA)
- Citywide Cybersecurity Categorization of Data and System Standard (S-03-ID-RA)
- Citywide Cybersecurity Categorization of Data and System Guidance (G-03-ID-RA)
- Citywide Inventory Policy (P-ID-AM-01)
- Citywide Encryption Policy (P-02-PR-DS)
- Citywide Encryption Standard (S-02-PR-DS)
- Citywide Cybersecurity Requirement for the Reuse and Disposal of Systems and Non-Computing Storage Devices Policy (P-04-PR-DS)
- Citywide Cybersecurity Requirement for the Reuse and Disposal of Systems and Non-Computing Storage Devices Standard (S-04-PR-DS)
- Mobile Computing Device Security Policy
- Portable Data Security Policy
- Agency Incident Response Plan (PR-IR-01)
- Citywide Incident Response Policy (P-PS-RP-01)
- 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 policies² 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 PrivacyOfficer@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 (**DORIS**). See [Section 5.7](#) for requirements on retaining identifying information.

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

City agencies should follow the Model Protocols for Handling Third Party Requests for Information Held by City Agencies (**Model Protocols**).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 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

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.

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 FOIL, 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 FOIL 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 FOIL requests by contacting a City agency directly or by submitting a request through the City’s FOIL portal ([OpenRecords Portal](#)), which is managed by DORIS.⁸ The OpenRecords Portal displays certain information about every FOIL 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 FOIL request via the OpenRecords Portal, it should determine whether the title 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 FOIL request titles from publication on the OpenRecords Portal for five business days. This delay purposefully coincides with the FOIL “acknowledgement period.”¹⁰ Agencies must determine whether to redact identifying information contained in the FOIL request title within this five-day period.

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.

¹⁰ [N.Y. Pub. O. Law § 89\(3\)\(a\)](#) grants entities subject to FOIL five business days to acknowledge receipt of a FOIL request.

- **Guidance Tip:** Each agency subject to FOIL 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 FOIL request where disclosure is not mandatory under FOIL, and a FOIL exemption is available but the agency is considering whether to disclose the information voluntarily. 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 now 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 personal information has been, or is reasonably believed to have been, accessed, acquired, disclosed, or used without authorization. Refer to [Section 8.0](#) 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.

¹¹ See Admin. Code § 23-501(g).

¹² *Id.*

¹³ See Admin. Code §§ 10-501(a) and (b).

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.

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

¹⁴ See Admin. Code § 23-1201.

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

[Charter § 8\(h\)\(4\)](#) empowers the Chief Privacy Officer to add types of information that are subject to the Identifying Information Law. The Chief Privacy Officer considers the nature of the information and the circumstances of its collection or potential disclosure. The Chief Privacy Officer has designated the following types of information:

- Date of birth
- Social Security number (including last 4 numbers)
- Taxpayer ID number (including last 4 numbers)
- Internet protocol address
- Device identifiers, including media access control (MAC) address or Internet mobile equipment identity (IMEI)
- GPS-based location obtained or derived from a device that can be used to track or locate an individual
- Palm and handprints
- Retina and iris patterns
- Facial geometry
- Gait or movement patterns
- Voiceprints
- DNA sequences

3.1.2 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 4.3](#) 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 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 Anonymized

“Anonymized” means having minimized or removed the elements of information that identify an individual. Anonymization includes other types of de-identification. See [Section 5.6.1](#) for additional guidance about anonymization.

3.2.3 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.

3.2.4 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,¹⁵ but agencies must have a process for receiving and investigating complaints.¹⁶

3.2.5 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.

3.2.6 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.

3.2.7 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. Agency privacy officers or the Chief Privacy Officer determine when identifying information is “sensitive identifying information.”

3.2.7.1 Requirements When Handling Sensitive Identifying Information

Sensitive identifying information is classified as “Restricted” information under the Citywide Cybersecurity Program Policies and Standards. 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.

¹⁵ Admin. Code § 23-1202(h).

¹⁶ Admin. Code § 23-1203(9).

3.2.8 “Requests” for Identifying Information

“Requests” for identifying information¹⁷ 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 for identifying information.

3.2.9 “Proposals” for Identifying Information

“Proposals” for identifying information¹⁸ means requests for identifying information for specific projects. Examples of “proposals” are projects for data integration, analysis, or 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 for identifying information.

3.2.10 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.¹⁹ Agencies must promptly notify the Chief Privacy Officer of the name and contact information for any new privacy officer by emailing PrivacyOfficer@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 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.

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 FOIL request.²⁰ Refer to [Section 1.6.1](#) on the relationship of FOIL to the Identifying Information Law.

¹⁷ See Admin. Code § 23-1205(a)(1)(c)(1).

¹⁸ See Admin. Code § 23-1205(a)(1)(c)(2).

¹⁹ See Admin. Code § 23-1201.

²⁰ See Admin. Code § 23-1201.

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.²¹ 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 PrivacyOfficer@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 reporting²² information about their policies.

Agency privacy officers must inform agency employees and covered contractors and subcontractors about this Policy and the Identifying Law.²³ 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.²⁴ 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.

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

²¹ See Admin. Code § 23-1202(g).

²² See Admin. Code § 23-1205.

²³ See Admin. Code § 23-1203(2).

²⁴ See Admin. Code § 23-1203(8).

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 disclosures of identifying information in violation of the Identifying Information Law.

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).

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 should consider the context in which their agencies collect and disclose identifying information and should adhere to the norms, roles, and purposes established by the context.

When considering whether to approve a collection or disclosure, agency privacy officers should fully understand the context, actors, attributes, and transmission principles that relate to the collection or disclosure. Agency privacy officers should not approve collections or disclosures that do not respect the “contextual integrity” of the identifying information.

- The context is the factual, legal, and social background conveying expected norms for how identifying information should be handled. Examples of contexts are law enforcement, outreach, health care, or social services. Consider both larger contexts (such as health care) and smaller contexts (such as encounters with physicians versus processing health insurance claims).
- Actors are the sender, recipient, and subject of identifying information.
- Attributes are the types or nature of identifying information. While attributes may be specified through data elements, agency privacy officers may instead specify attributes by referencing categories, such as demographic information as a whole.
- Transmission principles express the conditions under which identifying information is transferred. It includes conditions of confidentiality (such as that the recipient will not redisclose the identifying information), entitlement (such as that the sender is legally required to disclose the identifying information), and notice or consent (such as that the subject is aware of the collection or has consented to it).

• **Guidance Tip:** Considering whether people would be surprised to know how their identifying information is being collected, used, disclosed, or accessed can help illuminate the contextual integrity to be respected.

4.3.1 Pre-approval as Routine

Agency privacy officers may pre-approve collections or disclosures of identifying information as “routine.”²⁵ “Routine” approvals are necessary because agencies collect and disclose identifying information in their normal 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.

4.3.2 Approval on a Case-by-Case Basis of Collections and Disclosures That Are Not “Routine”

Agency privacy officers may, on a case-by-case basis, approve a collection or disclosure of identifying information if the collection or disclosure furthers the purpose or mission of the agency, or is required by law or treaty.²⁶ 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.

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.

4.3.3 Exemptions for Collections or Disclosures

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

4.3.3.1 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.²⁷

4.3.3.2 Exemption for Collections or Disclosures Involving Child Welfare Investigations

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.²⁸

²⁵ See Admin. Code §§ 23-1202(b)(2)(a) and (c)(2)(a).

²⁶ See Admin. Code §§ 23-1202(b)(1) and (c)(1).

²⁷ See Admin. Code § 23-1202(b)(2)(c) and (c)(2)(c).

²⁸ *Id.*

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 Chief Privacy Officer.²⁹ 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 and Collections or Disclosures Made Under Exigent Circumstances

Agency privacy officers are responsible for gathering information on any disclosures made in violation of the Identifying Information Law 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,³⁰ which means within 24 hours learning of violations of the Identifying Information Law or any 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,³¹ and makes them available [online](#).³² The quarters run as follows: June 16 through September 15th (1st Quarter); September 16 through December 15 (2nd Quarter); December 16th through March 15th (3rd Quarter); and March 16th through June 15th (4th Quarter).

4.4.2.1 Timing of Reporting Unauthorized Disclosures and Collections or 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 in violation of the Identifying Information Law, or collected or disclosed under exigent circumstances, even if the Chief Privacy Officer's report is not yet due.³³ Agency privacy officers should also notify the agency's general counsel of any suspected or known violation. 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 to 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.
- **Guidance Tip:** The agency may not have complete information about the unauthorized collection or disclosure or disclosure in 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, and may be made in any form.

²⁹ See Admin. Code § 23-1205.

³⁰ Admin. Code § 23-1202(c)(4).

³¹ See Admin. Code §§ 23-1202(c)(4) and (d)(2).

³² *Id.*

³³ See Admin Code § 23-1202(d)(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."³⁴ Second, they must "further the purpose or mission" of the agency.³⁵ 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.³⁶ 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 complementary 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."

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.

³⁴ See Admin. Code § 23-1201.

³⁵ *Id.*

³⁶ See Admin. Code § 23-1201.

➤ **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 4.2.1](#).

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 approvals.

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 either required by law or further the purpose or mission of the agency.³⁷

➤ **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, 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.³⁸ The Chief Privacy Officer may also approve *disclosures* of identifying information between City agencies in the best interests of the City.³⁹ Refer to [Section 5.2.3](#) on the Chief Privacy Officer’s role in non-routine collections and disclosures.

➤ **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.

³⁷ See Admin. Code § 23-1202(c)(3).

³⁸ See Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

³⁹ *Id.*

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:

- Is the collection or disclosure frequent or does it involve recurring action by the agency?
- Is the collection or disclosure made in the ordinary course of the agency’s daily business?
- Is the type of requesting entity involved with the normal business operations of the agency?

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 (see [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.

- **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) pre-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 as appropriate.

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:

- (1) the oversight agency is legally entitled to request the information;
- (2) the disclosing agency is not legally prohibited from disclosing the information to the oversight agency, and is not asserting a privilege; **and**

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

- (i) 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);⁴⁰ or
- (ii) the agency privacy officer approves the disclosure, on a case-by-case basis, as required by law; or
- (iii) the agency privacy officer approves the disclosure, on a case-by-case basis, as furthering the mission or purpose of the agency, subject to any necessary confidentiality agreements and data security requirements;⁴¹ or
- (iv) 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.⁴²

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 Cybersecurity Program Policies & Standards for handling information classified as “Restricted” information. Agencies should use a confidentiality agreement whenever possible even if the disclosure of sensitive identifying information is required by law. Agency privacy officer should seek guidance from the Chief Privacy Officer if they have difficulty obtaining an agreement.

- **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.

⁴⁰ See Admin. Code 23-1202(c)(2)(a).

⁴¹ See Admin. Code § 23-1202(c)(1)(b).

⁴² See Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

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 interest of the City.⁴³ Second, the Chief Privacy Officer can approve disclosures to City agencies upon determination that such disclosure is in the best interest of the City.⁴⁴

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. Agency privacy officers should consult with the Chief Privacy Officer for best interests of the City determinations.

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

5.3 Collections and Disclosures Involving Investigations

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.⁴⁵

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.⁴⁶

5.4 Collections and Disclosures Made Under Exigent Circumstances

Agencies may collect or disclose identifying information under exigent circumstances (refer to [Section 3.2.6](#) 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.

⁴³ See Admin. Code §§ 23-1202(b)(2)(b) and (c)(2)(b).

⁴⁴ *Id.*

⁴⁵ See Admin. Code §§ 23-1202(b)(2)(c) and (c)(2)(c).

⁴⁶ *Id.*

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.

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 Toolkit** for details).

➤ **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.

5.6 Data Minimization

Agencies should minimize the collection or disclosure of identifying information whenever possible. Agencies should balance privacy protection with their important work that requires cross-agency collaboration and coordination. Agencies should encourage employees to consult with agency privacy officers to figure out 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.

5.6.1 Anonymization

Anonymization means minimizing or removing the elements of information that identify an individual. Agency privacy officers should identify appropriate situations to anonymize information, considering their agencies’ purposes or missions and relevant laws. Agency privacy officers should work with technical staff to implement appropriate anonymization methods, which may include but are not limited to:

- **Aggregation:** Compiling data into a summary resulting in de-identification. For example, rather than sharing the names of each individual from a borough who applied for a program, an agency can state how many people from a borough were applicants.
- **Suppression:** Replacing data referring to a small number of individuals with a designated value. For example, if three public benefit recipients reside at the same address, an agency can replace “3” with “<5” or a symbol like “*” to denote the recipients. Agencies should generally suppress any identifying number less than 5 to protect against risks of identifying or locating individuals. Limiting disclosure of identifying information by using values of <5 through suppression, especially if sensitive identifying information is involved, may be particularly useful in public reporting or evaluation. Larger values may be appropriate in some contexts.

- *Pseudonymization*: Replacing identifying information with a non-identifying label so the information cannot be attributed to an individual (for example, replacing a person’s name with “A.”). Use caution when pseudonymizing data because simply re-labelling one type of identifying information will not be effective if the record contains many other types that could still re-identify the pseudonymized individual.
- *Redaction*: Removing identifying information before disclosing a record, such as by deleting birthdates from a document. When redacting, use methods that ensure the redacted text cannot be read. For physical copies, check both sides of the document. For electronic copies, check that the redaction cannot be removed.
- *Differential privacy*: Making available certain information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. When sharing sensitive statistical data, applying differential privacy techniques can help create a final dataset that does not reveal whether any one individual's identifying information was included in the original dataset.

➤ **Guidance Tip:** Other laws and regulations may define “anonymization” and “de-identification” differently from this Policy. Agency privacy officers should consult with the Chief Privacy Officer to determine the specific requirements in each context. They can also consult the Office of Technology and Innovation’s [Office of Data Analytics](#) for assistance with assessing datasets.

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.⁴⁷ 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 DORIS, 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 Cybersecurity Program Policies and Standards, the Citywide Technology Policies and Guidelines, 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

⁴⁷ Admin. Code § 23-1202(e).

Devices Policy and Citywide Cybersecurity Requirement for the Re-use and Disposal of Systems and Non-Computing Storage Devices Standard.⁴⁸ Agency privacy officers should work with records access officers 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.

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 contract provision related to the protection of identifying information.⁴⁹ 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.

The Identifying Information Rider was revised with version 3.0 of this Policy. The revision is effective **April 1, 2023**.

➤ **Guidance Tip:** If an agency believes that exceptional circumstances warrant modifying part of the Identifying Information Rider, it may modify the Identifying Information Rider only in consultation with the Office of Information Privacy.

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.⁵⁰ 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.⁵¹

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 (see [Section 3.2.7](#) 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](#).

⁴⁸ See Admin. Code §§ 10-503 and 10-504.

⁴⁹ See Admin. Code § 23-1203(7).

⁵⁰ See Admin. Code § 23-1201.

⁵¹ See Admin. Code §§ 23-1201 and 6-129(c)(21).

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 3.2.7](#) 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; or (ii) subcontracts for technology services that generally govern a contractor’s business relationships as a whole (i.e., for a broad range of clients, not just the City alone), provided that the City contractor includes appropriately protective privacy and security provisions in such subcontracts.

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

6.1.2.2 Contracts and Subcontracts for Outreach Services Involving Identifying Information

“Contracts and subcontracts for outreach services involving identifying information” include contracts and subcontracts where the contractor or subcontractor collects, uses, 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 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.

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. But data sharing agreements are generally not needed for “routine” disclosures 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 may include:

- sensitive identifying information;
- identifying information that is restricted by other laws or regulations;
- transferring custody and maintenance of identifying information to a third party; or
- 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 Toolkit** 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 required 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.

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.

7.3 Agency Implementation of Training Requirements

Agency privacy officers should identify personnel and 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 become aware of potential threats that could result in an incident or compromise the availability or integrity of identifying information to which that 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 for Violations of the Identifying Information Law

The Chief Privacy Officer accepts and investigates complaints of violations of the Identifying Information Law.⁵² 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

Agencies violate the Identifying Information Law when personnel or a covered contractor or subcontractor collect or disclose 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 per Admin. Code § 23-1202(c)(4) and [Section 4.4.2](#).

➤ **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. The protocol must, at a minimum:

- 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;⁵³ and

⁵² See Admin. Code § 23-1203(9).

⁵³ See Admin. Code § 23-1202(c)(4).

- Provide for other City offices to be engaged, including the Chief Privacy Officer, the Law Department, Cyber Command⁵⁴, and others that can help investigate the complaint and advise on a response.

A process for making complaints must be available to personnel and covered contractors and subcontractors. Agencies are encouraged to publish the protocols on their websites.

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. The Chief Privacy Officer will notify other City offices, such as the Law Department and Cyber Command, as necessary to coordinate further investigation and response.

8.3 Investigating Complaints

Agencies must have in place a plan for investigating complaints relating to a potential violation of 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 contact the Chief Privacy Officer as necessary for additional guidance.

8.4 Notification Requirements

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

- (1) Required by law or regulation;
- (2) 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
- (3) 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. 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.

⁵⁴ Not all complaints or incidents that impact privacy are cybersecurity matters. For suspected cybersecurity incidents, agencies and agency privacy officers should contact Cyber Command at by email at soc@oti.nyc.gov or soc@cyber.nyc.gov, or by phone at 718-403-6761. Cyber Command monitors these lines of communication at all hours.

Page Intentionally Blank

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

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

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

Page Intentionally Blank

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.	<ul style="list-style-type: none"> 3.2.2 Anonymization 5.6.1 Anonymization
2	Require the privacy officer of each City agency to issue guidance to City agency employees, contractors, and subcontractors regarding such agency’s collection, retention, and disclosure of identifying information.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 5.2.2.1 Requests Implicating Important Privacy Interests Including Sensitive Identifying Information 6.2.1 When an Agreement is Required
5	Describe disclosures of identifying information that are not to be treated as routine pursuant to section 23-1202, as determined by the nature and extent of such disclosures, and require an additional level of review and approval by the privacy officer of such agency or the contractor or subcontractor before such disclosures are made.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 6.1.1 Contracts and Subcontractors Subject to the Identifying Information Law 6.1.2.2 Contracts and Subcontracts for Outreach Services Involving Identifying Information 6.1.3 Non-Covered Contracts involving the Collection, Use, and Disclosure of Sensitive Identifying Information 6.2.2 Elements of Data Sharing Agreements 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 8.2 Receiving Complaints 8.3 Investigating Complaints

