

**MEMORANDUM OF UNDERSTANDING  
BY AND BETWEEN  
NEW YORK CITY DEPARTMENT FOR THE AGING  
AND  
NEW YORK CITY POLICE DEPARTMENT**

This Memorandum of Understanding ("MOU"), effective as of August 1, 2022 (the "Effective Date"), is made by and between the New York City Department for the Aging ("DFTA"), with offices at 2 Lafayette Street, New York, New York 10007; and the New York City Police Department ("NYPD"), with offices at One Police Plaza, New York, New York 10038 (together, the "Parties," and each a "Party").

**WITNESSETH:**

**WHEREAS**, Section 2402 of the New York City Charter gives DFTA the powers and duties to promote public awareness of resources available for the aging; to refer the public to appropriate departments and agencies of the city, state, and federal governments for advice, assistance and available services in connection with particular problems; to cooperate with and assist local neighborhoods in the development of programs and the establishment of local offices; and to serve as a clearing house for information relating to the needs of older adults; and

**WHEREAS**, DFTA has requested access to certain NYPD data in order to properly account for the servicing of older adult victims residing in Manhattan, to determine how many older adult victims are being serviced compared with those who are not, and to expand efforts to offer appropriate services to such older adult victims; and

**WHEREAS**, the NYPD has agreed to provide DFTA with certain data ("NYPD Data"), as defined herein, related to crimes wherein the victim is 60 years old or older with complaint reports occurring within the precinct boundaries of Patrol Borough Manhattan North and the 5<sup>th</sup> Precinct; and

**WHEREAS**, the New York City "Identifying Information Law," codified at Section 8(h) of the New York City Charter and Chapter 12 of Title 23 of the New York City Administrative Code ("Code"), sets forth procedures for the collection, retention, and disclosure of information obtained by or on behalf of New York City that may be used on its own or with other information to identify or locate an individual ("Identifying Information"); and

**WHEREAS**, the Parties are New York City agencies and subject to the Identifying Information Law; and

**WHEREAS**, Section 23-1202 of the Code provides that, absent exigent circumstances, agency employees may not collect or disclose identifying information without the approval of their Agency Privacy Officer ("APO"), and the data sought by DFTA contains Identifying Information related to older adult victims; and

**WHEREAS**, Section 23-1202 of the Code authorizes an agency's APO to approve collections and disclosure of Identifying Information that the APO has determined are "routine," meaning collections or disclosure that are made during the course of agency business and further the purposes of the mission of the agency; and

**WHEREAS**, the NYPD APO has not designated the disclosure of NYPD Data as "routine" and has an obligation, by law, to protect the privacy and security of Identifying Information; and

**WHEREAS**, Section 6.2.1 of the Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer ("CPO Policies") provides that "...when an agency makes a disclosure of identifying information to another agency that its [APO] has not designated as routine, the agency must enter into a data sharing agreement with the agency collecting the information unless the [APO], in consultation with the [CPO] as necessary, determines that such an agreement is not required because there is not a risk that an important privacy interest will be compromised" and expressly requires a data sharing agreement for data-sharing that involves the disclosure of "sensitive identifying information," as such term is defined in section 3.2.5; and

**WHEREAS**, Section 5.0 of the Citywide Information Classification Standard issued by the New York City Cyber Command requires that information must be classified as "Restricted" if the unauthorized disclosure of such information could be expected to have a severe or catastrophic adverse effect on, *inter alia*, individuals, and section 5.1 of the Cyber Command Citywide Information Management Standard requires that all information classified as Restricted shall be disclosed only to persons having authorized access and others with a business need to know who have signed a confidentiality or other legal agreement restricting re-disclosure of this information; and

**WHEREAS**, NYPD Data includes information that is classified under the Cybersecurity Standards as Restricted, and therefore the disclosure of NYPD Data to DFTA presents a risk that an important privacy interest may be compromised, and that any potential disclosure of the NYPD Data to unauthorized persons or entities would present a serious risk to the privacy, safety, and reputational interests of older adult victims; and

**WHEREAS**, the Parties seek to responsibly comply, in the context of NYPD disclosure to DFTA of NYPD Data as described herein, with both the law and New York City policies concerning the privacy and security of the NYPD Data.

**NOW, THEREFORE**, the Parties hereto agree as follows:

#### **ARTICLE I. TERM AND TERMINATION**

- A. This MOU shall commence as of the Effective Date and shall remain in effect for a period of three (3) years, from August 1, 2022 through July 31, 2025.
- B. Either Party may terminate this MOU upon thirty days' written notice to the other Party.

## **ARTICLE II. GENERAL PROVISIONS**

- A. The NYPD will provide to DFTA the following data in regards to crime victims over the age of sixty (60): anonymized complaint number; complaint precinct; classification of offense; jurisdiction description; report date; report command; incident date; classification; victim's first and last name; victim's age; victim's sex; victim's race; victim's email address; victim's home, cell, and business phone numbers; and the complaint narrative ("NYPD Data").
- B. The NYPD Data shall be limited to the scope of complaints occurring in the borough of Manhattan, specifically within the precinct boundaries of Patrol Borough Manhattan North and the 5<sup>th</sup> Precinct.
- C. DFTA shall designate an official custodian who shall be responsible for the maintenance, care, and security of the NYPD Data on behalf of DFTA (the "Official Custodian").
- D. NYPD shall provide the NYPD Data to DFTA beginning on August 1, 2022 and the NYPD Data shall subsequently be provided on a bi-weekly basis on Mondays for the term of this MOU. NYPD shall email notice of data readiness of the NYPD Data to the Official Custodian and Director of Elder Abuse Services.
- E. The NYPD shall share the NYPD Data with DFTA via secure means, including encryption and secure file transfer protocols, as described herein. NYPD Data shall be transferred electronically through an NYPD encrypted File Transfer Protocol Site ("FTP").
- F. The NYPD shall remain the data owner of the NYPD Data provided to DFTA under this MOU. If the NYPD instructs DFTA to destroy NYPD Data, DFTA will destroy it no more than five business days after receiving the instruction. DFTA will inform the NYPD that it has destroyed the NYPD Data no more than fifteen days after receiving the NYPD's instruction. If it is impossible for DFTA to destroy the NYPD Data, DFTA will explain in writing why it is impossible, and will, upon receiving the NYPD's destruction request, immediately stop accessing or using the NYPD Data and/or return the NYPD Data to the NYPD.

## **ARTICLE III. CONFIDENTIALITY OF NYPD DATA**

- A. DFTA shall maintain the security and confidentiality of all NYPD Data received in connection with this MOU, and shall comply with agency data security requirements, as well as all applicable provisions of federal, state, and local laws, rules and regulations, pertaining to confidentiality, privacy, and security of the NYPD Data received, generated, used, or held in the course of its performance under this MOU. Such safeguards shall include, but not be limited to, the following:
  - i. Access to NYPD Data in connection with this MOU is restricted to "Authorized Users" for a "Permitted Use."

- a. For purposes of this MOU, "Authorized Users" means DFTA employees, officials, and agents whose access to or use of the NYPD Data is necessary to execute their official job duties as they pertain to a Permitted Use.
  - b. For purposes of this MOU, "Permitted Use" means use of the NYPD Data by an Authorized User that is necessary to carry out that Authorized User's duties in relation to this MOU.
- ii. Except in connection with a Permitted Use in relation to this MOU, DFTA shall not use or disclose the NYPD Data without the NYPD's written permission, subject to Article III(A)(iv) below. DFTA will not use the NYPD Data for any purpose except as authorized under this MOU or as required by law. DFTA will limit access to NYPD Data to Authorized Users for the Permitted Use and will ensure that Authorized Users understand and comply with the provisions of this agreement applicable to NYPD Data;
- iii. DFTA will not use the NYPD Data for personal benefit or for the personal benefit of another, nor publish, sell, license, distribute, or otherwise reveal the NYPD Data without the prior written authorization of the NYPD;
- iv. Upon receipt of a subpoena, court order, request for NYPD Data pursuant to the Freedom of Information Law ("FOIL"), or other legal process served upon DFTA for NYPD Data, DFTA shall, within five (5) business days after it learns of the required disclosure, notify the NYPD, in order to allow the NYPD to seek a protective order and to make any required notifications, as appropriate. DFTA shall only disclose NYPD Data to the extent necessary to comply with the subpoena, court order, FOIL request, or relevant legal process;
- v. DFTA will use appropriate physical, technological, and procedural safeguards to protect the NYPD Data, including technically and physically limiting access to the NYPD Data on any DFTA computers, shared drives, laptops, or other devices and files, whether in paper or electronic format, to Authorized Users only, and utilizing secure means for accessing, storing, and transmitting the NYPD Data between and among Authorized Users;
- vi. DFTA will educate Authorized Users on their obligations under this MOU and applicable laws, regulations, and relevant New York City and agency policies;
- vii. DFTA will protect against anticipated hazards or threats to the integrity and security of the NYPD Data, and any unauthorized access to or disclosure of the NYPD Data, and shall take reasonable measures to prevent any other action that could result in harm to the NYPD and the individuals whose information DFTA is a recipient of; and

- viii. DFTA will comply with the New York City Information Technology Security Standards and Requirements, as set forth by the Department of Information Technology and Telecommunications and the NYC Cyber Command, and the CPO Policies, as they may be modified from time to time.
- B. All requests by third parties, including but not limited to governmental officials, commercial interests, researchers, and academics, for information exchanged between the Parties pursuant to this MOU shall be promptly communicated to the NYPD, including notification to the NYPD's APO.
- C. In the event of any breach involving the NYPD Data, DFTA shall: (i) advise the NYPD of the breach within 24 hours of discovery, including notification to the NYPD's APO; (ii) safeguard or destroy any information that would identify any individual, as requested by the NYPD; (iii) forward a written incident report to the NYPD expeditiously, and not re-disclose the identity of any individual to anyone else; and (iv) take reasonable steps to remediate the cause(s) of such breach, and provide written notice to the NYPD of such steps. For the avoidance of doubt, a breach is an occurrence or event which, intentionally or unintentionally, results in any of the NYPD Data being improperly released or removed from DFTA's custody.

#### **ARTICLE IV. USE OF AND ACCESS TO NYPD DATA**

- A. The NYPD shall encrypt the NYPD Data using a PGP 2048-bit encryption at rest in the NYPD Landing Zone. The NYPD shall transfer the NYPD Data to DFTA utilizing a secure, vetted data transfer protocol WinSCP or comparable system. The NYPD shall provide DFTA with a script and key file that will be used to decrypt the NYPD Data. If the key becomes compromised, DFTA must immediately notify NYPD so that a new key file may be generated. Authorized Users shall access the NYPD Data only through DFTA-issued devices with appropriate security safeguards, including, but not limited to:
  - i. Unique identification of authorized users utilizing WVD Multi-factor authentication ("MFA") or comparable system;
  - ii. Automated patch scanning and updating utilizing Desktop Central or comparable system;
  - iii. Vulnerability scanning utilizing Nessus or comparable system;
  - iv. Security monitoring utilizing Rapid 7 and Trustwave or comparable system;
  - v. Scans and monitoring of data leaving our network utilizing Forcepoint Data Loss Prevention ("DLP") or comparable system;
  - vi. Firewall configuration (unnecessary ports disabled); and

- vii. Scheduled automatic encrypted backups.
- B. The Official Custodian shall retrieve the NYPD Data and provide it to Authorized Users via a password protected file. Authorized Users will store the NYPD Data in a secure, password protected location ("Secure File"), and limit availability to Authorized Users.
- i. The Secure File shall not be accessible from a public-facing network.
  - ii. The Secure File is deleted within one (1) hour of successful retrieval by the Official Custodian.
  - iii. The NYPD Data is encrypted using Advanced Encryption Standard ("AES") 256 Algorithm at rest;
  - iv. Authorized Users shall be required to access the NYPD Data using a two (2) factor authentication to Windows Virtual Desktop ("WVD") and then an additional authentication; and
  - v. The Official Custodian shall ensure that the NYPD Data will be deleted from the Secure File in its entirety every two (2) weeks, unless any NYPD Data must be retained pursuant to Article III(A)(iv).
- C. Authorized Users shall be allowed to utilize the NYPD Data on the Secure File to initiate contact with victims.
- i. In the event that the victim consents to receive services offered by DFTA, Authorized Users shall be permitted to manually enter the NYPD Data outlined in Article II(A), with the exception of the complaint narrative, into DFTA's network.
  - ii. In the event that a victim declines services offered by DFTA, no NYPD Data shall be transferred to or stored on DFTA's network.
- D. Data retention policy for NYPD data loaded into DFTA's network is thirty (30) days. A user access log will be maintained by the NYPD for auditing purposes.
- E. DFTA shall ensure its network will comply with all applicable federal, state and local laws, statutes, acts, ordinances, rules, codes and regulations, executive orders and other official releases of or by any government, or any authority, department or agency thereof, including those in any jurisdiction from or in which the server is provided or received, including, but not limited to, those applicable to the privacy and protection of individuals, and the security of their personal information, including trans-border data transfers and data breach notification requirements.

- F. The Parties shall periodically assess the technological security of the NYPD Data to ensure that such security is consistent with the then-current information technology security standards and requirements of the City of New York.

#### **ARTICLE V. NO THIRD-PARTY BENEFICIARY**

This MOU shall be binding upon and for the benefit of, the successors, permitted assigns, executors and administrators of the Parties hereto. The provisions of this MOU shall be for the sole benefit of the Parties hereto and no other person or entity shall be a third-party beneficiary thereof.

#### **ARTICLE VI. MERGER AND MODIFICATION**

- A. This MOU constitutes the entire agreement between the Parties related to the subject matter of this MOU, and merges all prior discussions, agreements, or understandings into it. No prior agreements, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the Parties hereto.

- B. This MOU shall only be modified in a writing signed by both Parties.

#### **ARTICLE VII. NOTICES**

Except as otherwise provided herein, all notices required hereunder shall be in writing and directed to each of the Parties as follows:

If to NYPD:

New York City Police Department  
Deputy Commissioner, Community Partnerships  
One Police Plaza, Room 1404  
New York, NY 10038

With a copy to:

New York City Police Department  
Deputy Commissioner, Legal Matters  
Attn: Director, Privacy Matters  
One Police Plaza, Room 1406  
New York, NY 10038

If to DFTA:

New York City Department for the Aging  
Associate Commissioner, Bureau of Social Services and Direct Services  
2 Lafayette Street  
New York, NY 10007

With a copy to:

New York City Department for the Aging  
Director of Elder Abuse Services, Bureau of Social Services and Direct Services  
2 Lafayette Street  
New York, NY 10007

**IN WITNESS THEREOF**, the Parties have executed this MOU by the signatures of duly authorized officials.

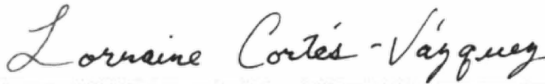
**NEW YORK CITY POLICE DEPARTMENT**



---

KEECHANT L. SEWELL  
Police Commissioner

**NEW YORK CITY DEPARTMENT FOR THE AGING**



---

LORRAINE CORTÉS-VÁZQUEZ  
Commissioner