

**Data Use and Non-Disclosure Agreement  
Between  
The New York City Department of Homeless Services and  
The New York State Department of Health**

This **DATA USE AND NON-DISCLOSURE AGREEMENT** (“Agreement”) made as of the January 14, 2023 (“Effective Date”) by and between the City of New York (“City”) acting by and through its Department of Homeless Services (“DHS”), having its primary offices at 33 Beaver Street, New York, New York 10004, and New York State Department of Health (“SDOH”), having its primary offices at Empire Plaza, Corning Tower, Albany, NY 12237, (each a “Party” and, collectively, the “Parties”).

**WHEREAS**, SDOH maintains the Statewide Planning and Research Cooperative System (“SPARCS”), a comprehensive all payer data reporting system which collects patient level detail on patient characteristics, diagnoses and treatments, services, and charges for each hospital inpatient stay and outpatient (ambulatory surgery, emergency department, and outpatient services) visit; and each ambulatory surgery and outpatient services visit to a hospital extension clinic and diagnostic and treatment center licensed to provide ambulatory surgery services; and

**WHEREAS**, under New York City Local Laws 114 & 115, DHS is required to use SPARCS data to prepare an aggregate health assessment report (“Health Report”), which will help DHS understand the pattern of health services usage among the DHS shelter and street homeless populations, how these patterns impact health outcomes, and to implement and inform interventions to reduce acute care use and improve health outcomes; and

**WHEREAS**, DHS has submitted a request to SDOH to receive SPARCS data pertaining to its clients (attached hereto as Exhibit \_\_\_\_\_), and has agreed to comply with SDOH’s Organizational Data Use Agreement and SPARCS Security Guidelines (attached hereto as Exhibit \_\_\_\_\_); and

**WHEREAS**, SDOH has agreed to match through its contracted provider DHS client data against SPARCS to retrieve patient level data related to DHS clients, and to share that data with DHS to allow DHS to prepare the Health Report, assess health patterns, and develop interventions; and

**NOW, THEREFORE**, in consideration of the mutual promises and covenants contained in this Agreement, and other valuable and good consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree to the following:

**I. TERM AND TERMINATION**

- A. **Term.** This Agreement shall commence as of the Effective Date and shall expire three (3) years thereafter, unless terminated earlier pursuant to this Section I.

The Parties may upon mutual agreement in writing extend this Agreement for an additional period not to exceed (3) years.

**B. Termination for Cause.** Breach of a material provision of this Agreement by either Party, or their Authorized Users (as designated pursuant to Section V(B)(1)) (the “Breaching Party”), shall be grounds for termination of this Agreement for cause by the non-breaching party (“Non-Breaching Party”). Upon becoming aware of such a breach of a material provision, the Non-Breaching Party may do one or more of the following:

1. Provide an opportunity for the Breaching Party to cure the breach or end the violation within thirty (30) days or such greater time period specified by the Non-Breaching Party, and terminate the Agreement if the Breaching Party does not cure the breach or end the violation within thirty (30) days or such other time period specified by the Non-Breaching Party;
2. Demand assurances from the Breaching Party that remedial actions will be taken to remedy the circumstances that gave rise to the breach or violation within a time frame set by, or approved by, the Non-Breaching Party;
3. Immediately terminate the Agreement; and/or
4. Determine that no further Data (as defined in Section III(A)) or other information will be released to the Non-Breaching Party for a period of time to be determined by the Non-Breaching Party.

**C. Termination without Cause.** Either Party may terminate this Agreement at any time by providing thirty (30) days written notice to other Party.

**D. Effect of Termination and Expiration.**

1. Upon the expiration or termination of this Agreement for any reason, the confidentiality provisions set forth herein shall continue to apply to the Data shared between the Parties pursuant to this Agreement. Except as provided in paragraph (3) of this subsection D, upon expiration or termination of this Agreement for any reason, each Party shall return or destroy the Data provided by the other Party and maintained in any form, and all copies of the Data in all its forms.
2. In the event that DHS or SDOH determines that returning or destroying all of the Data provided by the other Party, and all copies of that Data, is infeasible, DHS or SDOH shall provide notification of the conditions that make return or destruction infeasible to the other Party. Upon receipt by of such notification

that return or destruction of the Data is infeasible, the Parties shall extend the protections of this Agreement to such Data and limit further uses and disclosures of such Data to those purposes that make the return or destruction infeasible, for so long as the other Party maintains such Data.

## II. PURPOSE OF AGREEMENT

This Agreement sets forth the terms and conditions under which the Parties will permit access to and use of their Data, as defined in Section III(A) of this Agreement. This Agreement also describes in **Attachment B** what use each Party may make of the other Party's Data. Furthermore, this Agreement also sets forth the security requirements that such access and use is conditioned upon, including the responsibilities the Parties agree to assume in connection with such access and use of the Data, and all permutations of the Data, and the procedures for security, transfer, use, retention, ownership, and confidentiality of the Data.

## III. THE DATA

- A. **Definition of Data.** "Data" shall mean the data shared between the Parties pursuant to this Agreement and will include, without limitation, the specific description and data elements set forth in **Attachment A** to this Agreement.
- B. **Data Transmission.** The Parties shall securely transmit Data via the Aspera Secure File Transfer Protocol (SFTP). Once the data file has been transmitted, SDOH will provide a password by secure email.
- C. **Data Ownership.** Each Party retains sole ownership of its Data and all intellectual property rights therein. No license or conveyance of any such rights in the Data is granted or implied under this Agreement. Neither Party shall make, cause to be made, use or sell for any purpose any product or other item using, incorporating or derived from the other Party's Data, other than for the purpose stated in **Attachment B** for which such Data was provided under this Agreement. Either Party may at any time request that their Data be promptly returned or destroyed, unless determined to be infeasible as provided in Section I(D)(3) herein. Except as otherwise provided in Section I(D)(3) herein, upon written request by the other Party, DHS and SDOH shall promptly return or destroy (as requested) the Data provided by the other Party, and any notes, and other tangible materials representing such Data and all copies and reproductions thereof (in whole or in part) that may reside in their possession, including but not limited to, in or on their servers, computer systems, or files. As provided in

Section I(D)(3), where return or destruction is infeasible, the Data retained shall be protected as provided therein.

#### IV. PERMITTED USES OF THE DATA

- A. The Parties agree to use each other's Data solely for the purposes set forth in **Attachment B** to this Agreement, and for no other purposes.

Where a Party has been provided Data pursuant to this Agreement and the Data does not contain any identifying information, that Party shall not use the Data, either alone or in conjunction with any other information, in any effort to identify or locate any person to whom the Data relates. For the purpose of this subsection, identifying information shall have the same meaning as "identifying information" in Section 23-1201 of New York City Administrative Code.

#### V. **LEGAL BASIS FOR DISCLOSURE OF CONFIDENTIAL INFORMATION**

- A. Pursuant to NY Soc. Serv. Law § 136 and the implementing regulations at 18 NYCRR § 357.3(a), public assistance records and information relating to a person receiving public assistance and care may be disclosed by a public welfare official to another agency or person when the disclosure is reasonably related to the purposes of the public welfare program and the function of the inquiring agency, the confidential character of the information will be maintained, and the information will not be used for commercial or political purposes. The implementing regulations specifically permit disclosure of recipient-identifiable public assistance data for purposes directly connected to the administration of public assistance. 18 NYCRR § 357.2(a). For the administration of public assistance, federal regulations provide that the "use or disclosure of information concerning applicants and recipients will be limited to purposes directly connected with...establishing eligibility, determining the amount of assistance, and providing services for applicants and recipients." 45 CFR 205.50(a)(1)(i)(A). The sharing of the public assistance data under this Agreement would provide a service to DHS clients as it will assist DHS in their preparation and development of health assessment reports, health patterns and develop interventions. This will assist DHS to implement and inform interventions to reduce acute care and improve health outcomes for their clients.
- B. Pursuant to NY Public Officers Law § 96-a, the state and its political subdivisions may use or disclose a social security account number for internal verification, fraud investigation, or administrative purposes. DHS will disclose the last four digits of social security numbers to SDOH for the administrative purpose of facilitating an accurate data match that will facilitate this Agreement.

- C. Under New York City Administrative Code §23-1202(b) and §23-1202(c), the Agency Privacy Officer (APO) may designate in advance certain collections and disclosures of identifying information between City Agencies and/or third parties that further the purpose and mission of the agency as routine and therefore permissible. The APO of HRA/DSS agrees that the collection and disclosure of identifying information under this Agreement furthers the purpose and mission of DHS to assist with providing services to homeless individuals and families in New York City. The collection and disclosure of identifying information by DHS for the purposes set forth in this Agreement is covered by the following routine designation made by the HRA/DSS APO: Public Health and Safety, including Medical & Mental Health Services Reporting, Disease Prevention and Mortality Reporting.

## VI. CONFIDENTIALITY AND SECURITY OF DATA

### A. Compliance with Applicable Privacy and Security Laws, Rules, and Regulations.

The Data provided under this Agreement shall be used and maintained in accordance with applicable provisions of federal, state, and local laws, rules and regulations. In no case shall the safeguards listed above be less stringent than the safeguards set forth in the Citywide Privacy Protection Policies and Protocols of the Chief Privacy Officer, available at <https://www1.nyc.gov/site/moip/policy/the-policy.page>

### B. Restrict Access to “Authorized Users”.

1. DHS and SDOH shall restrict access to Data received under this Agreement to their employees, agents and/or contractors required to use the Data to perform the functions of this Agreement that are set forth in **Attachment B**, and so designated by the Parties as “Authorized Users” in **Attachment C** to this Agreement.
2. Each Party shall notify and train its Authorized Users as to the confidential nature of the Data and its proper handling.
3. The Parties certify that all Authorized Users will be subject to the obligations of confidentiality and non-disclosure no less stringent than those contained in this Agreement.
4. The Parties shall notify each other of any changes to the Authorized User list in **Attachment C** within five (5) days of any changes to the list.

5. The Parties shall immediately notify each other if any Authorized User has failed to comply with the terms of this Agreement and/or has compromised the privacy and security of the Data. Such conduct may result in the immediate removal of the user from the list of Authorized Users and the immediate termination of Data access to that specific user.

**C. Security and Confidentiality.** When a Party receives Data in accordance with this Agreement or creates and/or uses files derived from Data, that Party shall maintain the security and confidentiality of Data as required by this Agreement and applicable laws, rules and regulations. Except as otherwise provided in this Agreement, the Parties shall not, at any time, directly or indirectly, disclose, share, give, loan, sell, or otherwise grant access to the Data received pursuant to this Agreement, in part or in whole, to any other person or organization. For purposes of this Agreement, the terms “disclose” “disclosed” and “disclosure” in relation to Data shall have their ordinary meaning but shall be deemed to include providing access to, gaining access to, or being able to view, Data. Thus, an unauthorized disclosure of Data in violation of this Agreement will include an unauthorized party gaining access to or being able to view such Data. Without limiting this provision, the following confidentiality and security measures shall apply:

1. Disclosure of Individually Identifiable Information. The Parties shall not disclose Data, or any other information it receives pursuant to this Agreement, that is individually identifiable information, or information, which combined with publicly available information, may reasonably be used to identify an individual. Individually identifiable information must be maintained in accordance with this Agreement, and consistent with applicable laws, rules and regulations.
2. Reporting Unauthorized or Inadvertent Use or Disclosure.
  - a. In the event that a Party (the “Responsible Party”) either (i) reasonably suspects the occurrence of (a) any unauthorized or inadvertent use or disclosure of the Data by the Responsible Party, their employees, agents and/or contractors in violation of this Agreement, including, but not limited to, the theft or loss of portable devices or equipment containing the other Party’s Data or copies of Data, and/or (b) any unauthorized or inadvertent use or disclosure of the other Party’s Data resulting from hacking, software, malware, ransomware, computer code, algorithm or other means (each of item (a) and (b), an “unauthorized or inadvertent use or disclosure”), and

(ii) any remedial action to be taken by the Responsible Party with respect to such suspected occurrence of an unauthorized or inadvertent use or disclosure. The Responsible Party shall make such report to the designated privacy officer of the other Party (specified in, and per the Notice section of this Agreement), in writing, within three (3) business days after the Responsible Party becomes aware of such suspected occurrence of the unauthorized or inadvertent use or disclosure. The Responsible Party shall fully cooperate with any investigation conducted by the other Party or their agents to determine whether an unauthorized or inadvertent use or disclosure has occurred and the nature and extent of such unauthorized or inadvertent use or disclosure. The Responsible Party's full cooperation includes, but is not limited to, producing information requested by the other Party to enable the other Party to conduct an investigation of the suspected occurrence of the unauthorized or inadvertent use or disclosure.

- b. In addition to the requirements of the above paragraph (C)(2)(a), the Responsible Party shall provide notice to the other Party within three (3) business days of the discovery by the Responsible Party of any (i) breach of security, as defined in Section 10-501(b) of the New York City Administrative Code ("Admin. Code"), of any of the other Party's Data, encrypted or otherwise, that contains social security numbers or other "personal identifying information" as defined in Section 10-501 of the Admin. Code ("Personal Identifying Information"), where such breach of security arises out of the acts or omissions of the Responsible Party or their employees, agents or contractors, and/or (ii) any unauthorized or inadvertent use or disclosure of Data that contains any "protected health information" as defined in 45 CFR §160.103 ("Protected Health Information"), arising out of the acts or omissions of the Responsible Party or their employees, agents or contractors, and/or (iii) any unauthorized or inadvertent use or disclosure of Data that contains Personal Identifying Information and/or Protected Health Information resulting from hacking, software, malware, ransomware, computer code, algorithm or other means (each of item (i), (ii) and (iii), a "security breach"). Upon the discovery of any security breach, the Responsible Party shall take reasonable steps to remediate the cause or causes of such security breach and shall provide notice to the other Party of such steps. In the event of any

security breach, without limiting any other rights of the Parties, each Party shall be entitled to recover from the Responsible Party the costs of notifications and/or other actions mandated by the Admin. Code or any other applicable law, or administrative or judicial order, to address the security breach, including any fines or penalties imposed by the State or federal government as a result of the security breach. Each Party shall also be entitled to recover from the Responsible Party the costs of credit or identity theft monitoring services for individuals affected by such security breach by a national credit reporting agency, and/or any other commercially reasonable preventive or remedial measures. Each Party shall provide the Responsible with written notice and an opportunity to comment on such measures prior to implementation.

- c. The Parties shall comply with the above paragraph (C)(2)(b) as it pertains to Protected Health Information regardless of whether any of the Parties' use or disclosure of the Data is subject to the Health Insurance Portability and Accountability Act of 1996, and the regulations promulgated thereunder, as the law and regulations may be amended.

3. Accounting for Unauthorized or Inadvertent Use or Disclosure. In the event of an unauthorized or inadvertent use or disclosure of Data, the Responsible Party shall ensure that a proper record of such unauthorized or inadvertent use or disclosure is kept and immediately provided to the other Party. The Responsible Party shall also assist in any subsequent investigation of the unauthorized or inadvertent use or disclosure and mitigate any possible resulting damages of same. The record required under this provision, shall include, at a minimum:

- a. The date of the use or disclosure;
- b. The name of the user or recipient, if known;
- c. The address of the user or recipient, if known;
- d. A brief description of the information used or disclosed;
- e. Any remedial measures taken to retrieve or otherwise repossess such information or other measures to mitigate the use or disclosure of such information; and
- f. All other details required or necessary for the other Party to know when and how such unauthorized or inadvertent use or disclosure occurred and what mitigating steps are being undertaken or recommended by the Responsible Party.



**D. Safeguards to Protect the Data.** The Parties shall take all reasonable measures and ensure that all contractors take all reasonable efforts to safeguard and keep the Data confidential and secure, including, but not limited to:

1. storing the Data in secure access-restricted files;
2. using only DHS or SDOH issued or approved computers, laptops and/or mobile devices (collectively, "Devices") to access, process, transmit or store the Data;
3. encrypting any computer, laptop, USB, CD or other mobile storage tool, device, or equipment used to access, process, transmit or store the Data;
4. ensuring that only Authorized Users shall have access to the Data;
5. creating a password or encryption system to obtain and restrict access to the Data only to Authorized Users listed in **Attachment C**;
6. password protecting all Devices that will be used to access, process, transmit or store the Data;
7. keeping any hardcopy versions of files containing the Data in locked areas with access restricted to Authorized Users and maintaining a record of who accesses the hardcopy files;
8. keeping keys and combinations to locked areas protected from unauthorized access;
9. providing a firewall to protect Data so that no third party is allowed access to the Data;
10. whenever Devices that access, process, transmit or store the Data are left unattended for any length of time, access to such Devices must be immediately disabled, either manually or automatically, and a password must be required to access the Devices again;
11. adding tracking and remote data deletion software to all laptops and mobile devices that access, process, transmit or store the Data;

12. not leaving unattended laptops or mobile devices that are used to access, process, transmit or store the Data when transporting or traveling with the Data;
13. ensuring that all internal audit functions are reasonably maintained and operational; and
14. complying with any additional security requirements imposed by the other Party to ensure the security of the Data and minimize the risks of a breach.

E. **Security Audits.** DHS and SDOH reserve the right to demand prior to the transfer of their Data and periodically after the transfer of their Data copies of written, industry-standard audits and debriefings (in any format approved by DHS or SDOH) of the other Party's internal data safekeeping, data security technology, and other control systems ("security audits") conducted by the other Party or a third party, in order to provide reasonable assurance that the other Party is receiving and safekeeping the Data in compliance with the provisions of this Agreement and applicable laws, rules, and regulations. Upon request by the other Party, DHS and SDOH will promptly provide copies of such security audits and respond to inquiries regarding Data privacy and security. In addition to the foregoing, security audits may be conducted directly by DHS or SDOH or by a third party approved by DHS or SDOH. DHS and SDOH shall promptly provide the other Party or the third-party access to their internal systems for the purpose of conducting any security audit. DHS and SDOH shall immediately address all high and medium vulnerabilities identified by a security audit and implement a remediation plan and timeline which shall be provided to other Party.

F. **No Reproduction without Consent.** Except as provided in Section IV(A), DHS and SDOH shall not reproduce the other Party's Data in any form without the prior written consent of the other Party.

## VII. REQUIRED DISCLOSURE

Notwithstanding any inconsistent provision in this Agreement, the Parties shall not be liable for disclosure of the other Party's Data to the extent disclosure is required by virtue of court order, subpoena, other validly issued administrative or judicial notice or order, or pursuant to applicable law; provided that, in such event DHS or SDOH have given the other Party notice of its receipt of the court order, subpoena, other validly issued administrative or judicial notice or order, or request within five (5) days.

## VIII. REMEDIES FOR BREACH

A. DHS and SDOH acknowledge that:

1. a breach of this Agreement may cause the other Party irreparable damage for which recovery of damages may be inadequate.
  2. the damages flowing from such breach are not readily susceptible to measurement in monetary terms; and
  3. the other Party shall be entitled to seek immediate injunctive relief restraining any breach hereof, as well as such further relief as may be granted by a court of competent jurisdiction.
- B. Nothing in this Agreement shall be deemed to limit the Parties' remedies at law or in equity for any such breach by the other Party of any term of this Agreement.

## **IX. WAIVER**

Any waiver by DHS or SDOH of any act, failure to act or breach on the part of the other Party shall not constitute a waiver by DHS or SDOH of any prior or subsequent act or failure to act or breach by the other Party and shall not be effective unless set forth in a written document executed by the Parties.

## **X. INDEMNIFICATION**

- A. In no event will the DHS or SDOH be liable for any use or disclosure of the Data by the other Party, their employees, agents, and/or contractors, or for any claims, damages, losses, or liabilities, of whatsoever kind or nature, which may arise out of or in connection with the use or disclosure of the Data by the other Party, their employees, agents, and/or contractors.
- B. To the fullest extent permitted by law, each Party agrees to defend, indemnify and hold harmless the other Party (including their officials and employees) and their contractors, agents, and other members of its workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against any and all claims (even if the allegations of the claim are without merit), damages, losses, liabilities, and costs and expenses (including reasonable attorneys' fees) suffered by the Indemnified Party allegedly arising out of:
1. any failure by the other Party or their employees, agents, or contractors to comply with any of the provisions of this Agreement or with any applicable laws, rules or regulations, including the provisions relating to the use or disclosure of Data; or

2. any negligent act of commission or omission or intentional tortious act by the other Party or its employees, agents, or contractors.
- C. The Indemnified Party shall (i) make good faith efforts to provide timely written notice to the other Party of any claim for which indemnification is sought, (ii) permit the other Party to fully control the defense of any such claim, including, but not limited to, the selection of counsel and settlement, (iii) cooperate fully, at the other Party's expense, in the defense of such claim as requested, and (iv) not compromise or settle such claim without the other Party's written consent, which shall not be unreasonably withheld.
- D. Insofar as the facts or law relating to any of the indemnification obligations set forth above would preclude the Indemnified Party from being completely indemnified by the other Party, the Indemnified Part shall be partially indemnified by the other Party to the fullest extent permitted by law.

## **XI. NOTICE**

All notices under this Agreement shall be in writing and shall be deemed delivered as follows: (1) if by personal delivery or electronic mail, upon receipt; (2) if by Federal Express or by another national overnight courier, upon the second business day after deposit with such courier; or (3) if by US certified mail, return receipt requested, upon the fifth day after deposit in the mail. All notices shall be sent to the names and addresses set forth below. Either Party may change its contact information by notice to the other; any such change shall take effect immediately upon delivery of such notice. Any notice pursuant to this Agreement shall be given or made to the respective Parties as follows:

For DHS:

New York City Department of Homeless Services

33 Beaver Street

New York, NY 10004

Attn: Fabienne Laraque

Cc: Lauren Friedland, DHS Chief Privacy Officer (for breach notifications)

For New York State Department of Health:

New York State Department of Health

Empire State Plaza, Corning Tower, Room 1911

Albany, New York 12237

Attn: Jim Kirkwood  
Cc: Ken Wiczerza, APD Policy and Privacy Advisor

## **XII. PUBLICATION AND PUBLIC RELEASE OF DATA**

- A. The Parties shall not reveal any individually identifiable information received pursuant to this Agreement, such as a person's first or last name, date of birth, or any other identifying information, in any draft or final publication.
- B. DHS and SDOH must obtain prior written approval from the other Party before releasing to the public any information concerning this Agreement.

## **XIII. MERGER CLAUSE**

This Agreement and the Attachments hereto constitute the entire understanding of the Parties and merges all prior discussions, agreements or understandings into it. No prior agreement, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the Parties.

## **XIV. MODIFICATION**

- A. This Agreement may, from time to time, be modified by a writing signed by authorized representatives of the Parties. It may not be altered, modified, rescinded or extended orally.
- B. The Attachments hereto may be modified upon written agreement by the Parties without the need to formally amend this Agreement. Each attachment that is modified shall be deemed to be part of this Agreement and will supersede any prior Attachment, or Attachment modification, as applicable. Upon the modification of any Attachment, all references in this Agreement to such attachment shall be deemed to be references to the Attachment as modified.

## **XV. NON-ASSIGNMENT CLAUSE**

The Parties agree that it shall not subcontract, assign, transfer, convey or otherwise dispose of their obligations under this Agreement without the prior written consent of the other Party.

**XVI. NO THIRD-PARTY BENEFICIARY**

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties, any rights, remedies, obligations, or liabilities whatsoever.

**XVII. ADDITIONAL PROVISIONS**

- A. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of New York (without regard to choice of law or conflict of law principles) and the laws of the United States, where applicable.
- B. **Jurisdiction and Venue.** The Parties agree that any and all claims arising under or related to this Agreement shall solely be heard and determined either in the courts of the United States located in the City of New York or in the courts of the State of New York located in the City and County of New York.
- C. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement. This Agreement may also be executed in counterpart facsimile or scanned signatures, each of which facsimile or scanned signature of a Party shall be deemed to be the original signature of such Party.
- D. **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Parties to maintain the confidentiality and security of the Data.
- E. **Headings.** The headings and other captions in this Agreement are for convenience and reference only and shall not be used in interpreting, construing or enforcing any of the provisions of this Agreement.
- H. **Severability.** If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole and, in such event, such provision shall be changed and interpreted so as to best accomplish the objectives of such unenforceable or invalid provision within the limits of applicable law or applicable court decisions.
- I. **Survival.** Upon the expiration or earlier termination of this Agreement, the continued use of Data for the purposes set forth in **Attachment B** shall cease. All other provisions of this Agreement shall survive.

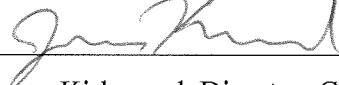
**IN WITNESS WHEREOF**, and intending to be legally bound, the Parties hereto have executed this Agreement as of the day and date first written above.

NEW YORK CITY DEPARTMENT OF HOMELESS  
SERVICES

By: \_\_\_\_\_

Vincent Pullo, Agency Chief Contracting Officer

NEW YORK STATE DEPARTMENT OF HEALTH

By:  \_\_\_\_\_

James Kirkwood, Director, Center for Health Data  
Innovation

## Data Use and Non-Disclosure Agreement

### ATTACHMENT A – DATA POINTS

In accordance with Section III(A) of this Agreement, Data shall mean the data shared between the Parties pursuant to this Agreement and will include, without limitation, the specific description and data elements set forth below:

#### A. DHS Data

DHS shall provide the following data elements for all DHS clients from 2017 to the present

- Enhanced Unique Personal Identifier (EUPI) which includes the following data elements:
  - 1) First two letters of the Last Name
  - 2) Last two letters of the Last Name
  - 3) First two letters of the First Name
  - 4) Last four digits of the Social Security Number (If not available, use 0000)
  - 5) Date of birth (YYYYMMDD)
  - 6) Gender (M/F/U)
  
- CARES ID

#### B. SDOH Data

Any of the inpatient SPARCS data elements listed on SDOH's website at:

<https://www.health.ny.gov/statistics/sparcs/sysdoc/inpatientoptoc.pdf>

- Any of the outpatient SPARCS data elements listed on SDOH's website at:

<https://www.health.ny.gov/statistics/sparcs/sysdoc/outpatientoptoc.pdf>



## **Data Use and Non-Disclosure Agreement**

### **ATTACHMENT B – Project Description and Data Use**

In accordance with Section IV(A) of this Agreement, DHS and SDOH agree to use the Data provided by the other Party under this Agreement solely for the purposes and project set forth below, and for no other purposes:

- I.** DHS will share a list of EUPIs and CARES ID for each client in its CARES database with SDOH; this list will be transferred to SDOH via Aspera or another mutually agreed-upon secure file transfer protocol (SFTP)
- II.** SDOH will transmit the list of EUPIs and CARES IDs via SFTP to Optum Government Solutions, Inc., the contracted vendor for SPARCS data intake, processing, and extractions.
- III.** Optum staff will use the EUPIs provided by DHS to conduct a match against SPARCS to retrieve patient level health services information about DHS clients in the CARES database
- IV.** Optum will remove the EUPIs from the list of DHS clients, and return the patient level health services information associated with each CARES ID back to SDOH via SFTP.
- V.** SDOH will transfer the patient level health services information associated with each CARES ID back to DHS via Aspera or another mutually-agreed upon SFTP.
- VI.** DHS will use the information provided by SDOH to prepare a Health Report as required by NYC Local Law 114 and may use the information to understand the pattern of health services usage among the DHS shelter and street homeless populations, how these patterns impact health outcomes, and to implement and inform interventions to reduce acute care use and improve health outcomes.





