



Department of Health

ANDREW M. CUOMO
Governor

**HOWARD A. ZUCKER, M.D.,
J.D.**
Commissioner

SALLY DRESLIN, M.S., R.N.
Executive Deputy
Commissioner

Dear:

Michele Warner

Enclosed please find the New York State Department of Health (DOH), Office of Health Insurance Programs (OHIP), Medicaid Confidential Data (MCD) Data Use Agreement (DUA).

The purpose of the DUA is to provide a means for the Requesting Organization (Requestor) to provide information to allow DOH to support a request for the release of MCD to the Requestor.

In addition, the DUA establishes a legally binding agreement between the Requestor and DOH by defining the terms and conditions of the MCD release, should DOH accept the Requestor's Agreement. *The sensitivity of MCD cannot be over-emphasized. MCD includes all personal information about Medicaid recipients, including Protected Health Information (PHI).*

Furthermore, if the Requestor plans to hire subcontractors to work with MCD, the Requestor must complete and submit a DUA Addendum along with the Business Associate Agreement (BAA) to DOH. DOH must acknowledge the acceptance of the DUA Addendum and BAA to the Requestor before the subcontractor may access MCD.

The Requestor is responsible for complying with all federal and state laws and regulations regarding the privacy, protection, and security of MCD.

Please fill out this DUA in its entirety and be sure to attach all required supporting documentation. Send completed scanned applications to:

Email:
doh.sm.Medicaid.Data.Exchange@health.ny.gov
Security and Privacy Bureau
Division of Operations and Systems
Office of Health Insurance Programs
New York State Department of Health

Please contact the email address above if there are any additional questions about this agreement or Medicaid's data security requirements.

Section 1: Requestor Information

- I. This Agreement is by and between the New York State Department of Health (DOH), and the New York City Human Resources Administration/Department of Social Services (HRA or DSS), being signed for by, Karen Lane , an authorized individual of the Organization, hereinafter termed "Requestor".
- II. Provide the name, title and contact information of the individual authorized to legally bind your company, agency or entity to the terms of this Agreement. The person who is named in this section must sign all sections of the Data Use Agreement (DUA), except for the Custodian section which must be signed by the Custodian(s).

Authorized Individual:	Karen Lane
Title:	Executive Deputy Commisstioner
Organization:	HRA Medical Insurance Community Servoces Administration (MICSA)
Address:	4 World Trade Center, 150 Greenwich Street, New York, NY 10007
Telephone:	929-221-2565
Email Address:	lanek@dss.nyc.gov
Contract or Grant Number:	Sponsorship
Entity Type:	☐ Qualified Entity (QE) ☐ Health Home (HH) ☐ Performing Provider System (PPS) ☐ Value Based Payment (VBP) Participant ☐ Managed Care Organization/Plan (MCO/MCP) ☐ State Entity: Click or tap here to enter text. ☒ Other: NYC HRA

- III. DOH agrees to provide the Requestor with MCD from the DOH Medicaid Data Warehouse (MDW) or other recognized DOH data source. In exchange, the Requestor agrees to use the MCD only for purposes that support the Requestor's project, research or study referenced in this Agreement, which DOH has determined assists in the administration, monitoring, management and improvement of the State Medicaid program or the services provided to beneficiaries. The Requestor agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity and availability of the MCD by complying with the terms of this Agreement, State and Federal law, including the Health Insurance Portability and Accountability Act (HIPAA), NIST 800-53 Rev. 4, and NYS Information Security Policy P03-002.
- IV. This Agreement contains the terms and conditions under which DOH will disclose, and the Requestor will obtain, use, reuse, disclose and destroy the DOH MCD data file(s) specified in Section 3: Data Description. This provision also applies to all derivative or commingled file(s) that contain direct individual identifiers or elements that can be used to identify specific individuals when used in concert with other information. This Agreement supersedes all agreements by and between the parties with respect to the use of MCD from the files specified in Section 3 and preempts and overrides any

previous instructions, directions, agreements, or other prior communication from the DOH or any of its components with respect to the data specified herein.

Section 2: Purpose

- I. In consideration for accepting the data file(s), the Requestor represents that such data file(s) will be used solely for the purpose(s) listed below. Requestor agrees not to disclose, use or reuse MCD for any purpose, other than as described herein, without an executed and accepted DUA Addendum by and between Requestor and DOH. The Requestor affirms that the data requested by the Requestor is the minimum necessary to achieve the purposes stated in this section. The Requestor agrees that, within the Requestor's Organization and the organizations of its business associates, access to the data covered by this Agreement shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated in this section.
- II. In this section, Requestor should describe the purpose of the project, as well as how MCD will be used to assist DOH in the administration, monitoring, management and improvement of the New York State Medicaid program or the services provided to beneficiaries. The description of the project should clearly state the purpose of the initiative.

The Office of Evaluation Research and Policy (OER) is HRA's research and policy unit that provides analysis for and directly advises the Commissioner of DSS, the Administrators of HRA and Department of Homeless Services (DHS), various deputy commissioners, and the heads of HRA and DHS program areas. OER uses administrative data and other resources to provide analysis of HRA and DHS programs and policies to inform decisions and strategic planning at multiple levels throughout the agencies. OER would use confidential Medicaid data in the MDW solely for the purpose of answering specific research questions posed by internal DSS/HRA/DHS policymakers.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Section 3: Data Description

- I. The following DOH data file(s) or data elements, not to exceed the minimum necessary standard, are requested under this Agreement:
 - A. Specify the individual Medicaid record level data elements needed for this request:

OER will need individual level identifiers for data matching (e.g., to HRA Welfare Management System [WMS]), such as SSN, First Name, Last Name and DOB. We will also need basic case data, including MA Eligibility Dates, Coverage Information, Provider, and Demographic Information.
 - B. Specify the dates of the data requested:

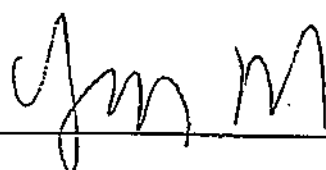
Last 5 years.
 - C. Specify the frequency and schedule of data release:

Monthly.

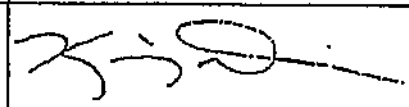
Section 4: Custodian

- I. The parties mutually agree that the following named individual(s) is (are) designated as Custodian(s) of the file(s) on behalf of the Requesting Organization and will be the person(s) responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The Custodian(s) agrees to notify DOH within fifteen (15) days of any change of custodianship. The parties mutually agree that DOH may disapprove a custodian or may require the appointment of a new custodian at any time. The Custodian(s) hereby acknowledges his/her appointment as Custodian(s) of the aforesaid file(s) and agrees to comply with all of the provisions of this Agreement on behalf of the Organization. Should there be a third-party contractor in possession of MCD on Requestor's behalf, they, too, must designate a Custodian and submit the Custodian to DOH for acceptance.
- II. Custodian(s), also known as Gatekeepers, shall be responsible for providing access to, and accurately documenting, certain information related to workforce members who access MCD on behalf of the requesting entity. Custodians must accurately record all entity staffing changes, and provide a quarterly report ("Quarterly Names Update") to the Security and Privacy Bureau containing the first and last names, and employment start and end dates of all affected employees.
- III. Custodians must also provide this report upon written request from DOH. This quarterly report must always be accompanied by a notarized DUA Addendum. In addition to the Quarterly Names Update, Custodians must notify the Security and Privacy Bureau, within 24 hours, any time an employee or subcontractor joins or leaves the Requesting Organization. All Custodian changes also require the submission of a notarized DUA Addendum to DOH.
- IV. Requestor or Custodian shall provide all policies and procedures related to workforce system access management including provisioning, modifying, and terminating users who access any system that stores, processes, analyzes or transmits MCD on behalf of the Requesting Organization.
- V. Lead Custodian:

NYSDOH OHIP Data Use Agreement #: Click or tap here to enter text.

Lead Custodian:	Grace Zhang
Title:	DSS Chief Information Security Officer (CISO)
Organization:	New York City Department of Social Services
Address:	250 Church Street, 10 th Fl, New York, NY 10050
Telephone:	718-510-0550
Email Address:	ciso@dss.nyc.gov
Date of Signature	Click or tap to enter a date. 8/8/18
Signature:	

VI. Alternate Custodian:

Alternate Custodian:	Kinsey Dinan
Title:	Deputy Commissioner
Organization:	New York City Department of Social Services Office of Evaluation and Research
Address:	150 Greenwich Street, 42 nd Floor, New York, NY 10007
Telephone:	929-221-7349
Email Address:	dinank@dss.nyc.gov
Date of Signature	5/2/2018
Signature:	

Section 5: Security

- I. The Requestor warrants that it shall employ appropriate administrative, technical, and physical safeguards to protect the confidentiality and security of data provided under this DUA. The safeguards employed shall provide a level and scope of security that is not less than the level and scope of security requirements established by Federal and New York State policies. Further, the Requestor agrees that the data must not be physically moved, transmitted, or disclosed in any way from or by the site indicated in Section 6: Data Storage and Access without written approval from DOH.
- II. DOH shall, at its sole discretion, require Requestor to complete and submit Moderate-Plus System Security Plan (SSP) Workbooks, a System Security Plan Controls Attestation, or establish a Restricted Access Model (RAM) Environment for any system(s) that will store, process or permit access to MCD. DOH shall evaluate Requestor's DUA submission, determine the most appropriate solution for securing MCD, and provide Requestor with necessary materials to fulfill this requirement.

Section 6: Data Storage and Access

- I. When Requestor and Custodian take possession of MCD, it shall be stored in the location specified below. The data cannot be transferred by any means to another environment without a DUA Addendum to this Agreement that has been accepted by DOH.

Type of Storage Environment:	☐ Restricted Access Model ☒ Production ☒ DOH System Access: MDW ☐ Other: Click or tap here to enter text.
Title of Location:	4 Metrotech
Company Housing Data:	NYC Department of Social Services, ITS
Address of Location:	150 Greenwich St., New York, NY 10007

Section 7: End Date and Destruction of Data

- I. The parties mutually agree that the aforesaid file(s) (and/or any derivative file(s)), including those files that directly identify individuals, may only be retained by the Requestor until December 31, 2021, hereinafter known as the "End Date." The DUA may only be extended past the End Date if a written DUA Addendum is accepted by DOH prior to the DUA expiration date. Extensions of the DUA will be tied to: A) end dates of contracts with DOH; B) end dates for Centers for Medicare and Medicaid Services (CMS) grants; or C) per OHIP sponsor determination.
- II. If the purpose described in Section 2: Purpose is completed prior to the End Date, the Requestor agrees to notify DOH within 30 days of completion. Upon such notice or the End Date, whichever occurs sooner, the Requestor agrees to destroy all data provided under this DUA, unless DOH grants an exception. If DOH grants the exception, the MCD must be protected until it has been destroyed. The Requestor agrees to destroy all MCD and submit a Data Destruction Affidavit to DOH within 30 days of the project completion. The Requestor agrees not to retain any DOH MCD files or any parts thereof, unless authorized in writing by DOH. DOH does not have to notify Requestor of the End Date for this provision to apply. Either party may terminate this DUA at any time, for any reason, upon 30 days written notice to the other party. Upon notice of termination by Requestor, DOH will stop releasing data file(s) to the Requestor and the Requestor must destroy all data file(s) Requestor has already received. If a Data Consuming Entity (DCE) goes out of business it shall destroy all MCD it has received from DOH and submit a Data Destruction Affidavit to DOH within 30 days.

Section 8: Offshore Prohibition

The Requestor further agrees that any MCD provided under this Agreement shall not be accessed by employees, agents, representatives, or contractors who are located outside of the United States and its territories (offshore). Further, the Requestor agrees that MCD shall not be received, stored, processed, or disposed via information technology systems which are located offshore.

Section 9: Unauthorized Use or Disclosure, Breach and Incident Response

- I. The Requestor agrees that if DOH determines or believes that the Requestor has used, reused or disclosed MCD in a way other than as explicitly authorized by this Agreement, DOH may, at its sole discretion, require the Requestor to:
 - A. Promptly investigate and report to DOH the Requestor's determinations regarding any alleged or actual unauthorized use, reuse or disclosure;
 - B. Promptly resolve any problems identified by the investigation;
 - C. If requested by DOH, submit a formal response to an allegation of unauthorized use, reuse or disclosure;
 - D. If requested by DOH, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and
 - E. If requested by DOH, destroy all data files received from DOH and submit a Data Destruction Affidavit. The Requestor understands that upon DOH's determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, DOH may suspend further release of MCD to the Requestor, indefinitely. The Requestor agrees to report any breach of personally identifiable information (PII) or Protected Health Information (PHI) from the DOH data file(s), loss of MCD or disclosure to any unauthorized persons to the DOH by e-mail notification at doh.sm.Medicaid.Data.Exchange@health.ny.gov within one hour of discovery, and to cooperate fully in the security incident investigation and review process. While DOH retains all ownership rights to the data file(s), as outlined above, the Requestor shall bear the cost and liability for any breaches of PII or PHI from the data file(s) while they are entrusted to the Requestor. Furthermore, if DOH determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the Requestor agrees to carry out these notifications without any cost to DOH.
- II. If Requestor determines that an incident has occurred in one of Requestor's systems, Requestor must notify DOH. An incident is defined as violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. DOH may require Requestor to complete a risk analysis, risk assessment and an organizational attestation affirming that Requestor has identified and remediated the root cause of the malicious software outbreak, cyberattack, or other information security incident and that Requestor's systems and networks have been remediated and have returned to normal operation. Requestor understands that access to DOH systems will not be granted until the organizational attestation is completed and accepted by DOH. Requestor acknowledges that Requestor's organization is liable if ransomware or malware spreads to DOH systems from Requestor's systems.
- III. Prior to the start of forensic activities related to significant information security incidents, the organization should determine how it will collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. The organization should make all such forensic decisions in accordance with its policies and advice from legal counsel. In such situations, the organization should follow a clearly defined chain of custody to avoid allegations of mishandling or tampering with evidence. The organization should keep a log of every person who had physical custody of the evidence, and document the date and time of the actions that they performed. The organization should make a forensic copy of the evidence and verify the integrity of both the original and the copied evidence. The organization should assure that the original evidence is stored securely and perform all forensic examination and analysis using only the copied evidence. If it is unclear whether or not evidence preservation is required, the evidence should be preserved. All forensic examination, such as that described above, must account for the disposition and impact on

all DOH data as well as all systems that store, process, analyze, or transmit DOH data in the report provided to DOH.

Section 10: HIPAA Business Associate Agreement

Complete and return Attachment A: HIPAA Business Associate Agreement along with the DUA application.

Section 11: Sharing Data with Third Parties

- I. Requestor agrees not to share MCD obtained from DOH with other parties unless DOH has accepted a DUA Addendum and a copy of the Business Associate Agreement (BAA) executed between Requestor and the third-party Business Associate with DOH. Any BAA submitted for DOH acknowledgement as part of a DUA addendum must contain at minimum the confidentiality language found in part II.
- II. Confidentiality Language for Third Parties.
 - A. The Federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive MCD must include contract language that will bind such parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data. This notification requires that you include the following language in this contract and all future contracts that will govern the receipt and release of such confidential data:
 1. Medicaid Confidential Data/Protected Health Information includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.
 2. You must comply with the following state and federal laws and regulations:
 - a. Section 367-b(4) of the NY Social Services Law
 - b. New York State Social Services Law Section 369(4)
 - c. Article 27-F of the New York Public Health Law and 18 NYCRR 360-8.1
 - d. Social Security Act, 42 USC 1396a(a)(7)
 - e. Federal regulations at 42 CFR 431.302 and 42 CFR Part 2
 - f. The Health Insurance Portability and Accountability Act (HIPAA) and HITECH, at 45 CFR Parts 160 and 164
 - g. NYS Mental Hygiene Law Section 33.13
 - B. Please note that MCD released to you may contain AIDS/HIV related confidential information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5)(a), the following notice is provided to you: "This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."
 - C. Alcohol and Substance Abuse Related Confidentiality Restrictions: Alcohol and substance abuse information is confidential pursuant to 42 CFR Part 2. General

authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

- D. You agree to ensure that you and any agent, including a subcontractor, to whom you provide Medicaid Confidential Data or Protected Health Information (MCD/PHI), agrees to the same restrictions and conditions that apply throughout this Agreement. Further, you agree to state in any such agreement, contract or document that the party to whom you are providing the MCD/PHI may not further disclose it without the prior written approval of the New York State Department of Health. You agree to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that you enter into that involves MCD/PHI.
- E. Any agreement, contract or document with a subcontractor must contain all of the above provisions pertaining to confidentiality. It must contain the HIV/AIDS notice as well as a statement that the subcontractor may not use or disclose the MCD without the prior written approval of DOH.

Section 12: Publications

The Requestor agrees not to disclose direct findings, listings, or information derived from the file(s) specified in Section 3, with or without direct identifiers, without the express written consent of DOH, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. The Requestor further understands and acknowledges that any publications derived from MCD must be reviewed and approved by the DOH prior to publication or public release. The term publication is defined to include, but is not limited to: written abstracts, articles and papers; presentations at conferences, board meetings, r advisory committee meetings, task forces, or collaborative groups; minutes of meetings, charts, graphs, data sheets, and slides; posting of information on a website, or social media such as Facebook, LinkedIn, Twitter; or email. DOH Office of Health Insurance Programs (OHIP) requires at least forty-five (45) business days to review and approve proposed publications. Any research publication shall include the following disclaimer: "Disclaimer: The views and opinions expressed in this article are those of the author(s) and do not necessarily reflect the official policy or position of the New York State Department of Health. Examples of analysis performed within this article are only examples. They should not be utilized in real-world analytic products."

Section 13: Attestation and Execution

- I. By signing this Agreement, the Requestor and Custodian agree to abide by all provisions set out in this Agreement and acknowledges that violation of the terms of this Agreement may have potential civil, criminal or administrative penalties.
- II. By signing this Agreement, the Requestor agrees to grant access to MCD at any time to authorized representatives of DOH at the site indicated in Requestor's SSPs or RAM documentation for inspecting and confirming compliance with the terms of this Agreement.
- III. By signing this Agreement, the undersigned individual hereby attests that he or she is authorized to enter this Agreement and legally bind the organization and agrees to all the terms specified herein.
- IV. By signing this Agreement, the Requestor agrees that this Agreement shall be deemed executory to the extent of the resources available to DOH Medicaid program and no liability on account thereof shall be incurred by the DOH Medicaid beyond the resources available thereof.

- V. The parties mutually agree that DOH retains all ownership rights to the data file(s) referred to in this Agreement, and that the Requestor does not obtain any right, title, or interest in any of the MCD furnished by DOH. DOH reserves the right to require Requestor to destroy all MCD received from DOH any time and for any reason. If DOH exercises this right and requires Requestor to destroy all MCD received from DOH, a Data Destruction Affidavit form must be completed and returned to DOH.
- VI. By signing this Agreement, the Requestor agrees to be responsible for the use of MCD, whether the data is in its hands or in the hands of its contractors/subcontractors. Requestor will also be responsible for the establishment and maintenance of security, to prevent unauthorized use of MCD. The Requestor represents and warrants that such data will not be disclosed, released, revealed or showed, or access granted to any person other than those listed on the Names List provided to DOH. Any improper use or disclosure of MCD must be reported to the Security and Privacy Bureau. Requestor agrees to establish and ensure that its contractors/subcontractors, if any, establish appropriate administrative, technical and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use of or access to the data. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Federal Health Insurance Portability and Accountability Act of 1996. There should be no release of MCD unless written permission is received from DOH.
- VII. Attestation Regarding Privacy/Security of Medicaid Confidential Data: Requestor, contractors and subcontractors hereby agree to all confidentiality language for Third Party Contractors found in Section 11: Sharing Data with Third Parties of the DUA, and that these citations must be included in all MOU, MOA, Subcontracts or Contracts. Requestor, contractors and subcontractors hereby acknowledge that all subcontractors will be listed in a DUA Addendum, and that a BAA will be maintained by the contractor and provided to DOH.
- VIII. Limitations and Liabilities: DOH will not be responsible for any loss due to data exchange.
- IX. Assignment: The Requestor may not assign, transfer, convey, or sublet, directly or indirectly, all or part of its rights or obligations under this Agreement.
- X. This Agreement shall be governed by and interpreted in accordance with the laws of the State of New York. If any provision of this Agreement conflicts with any statute or rule of law of the State of New York, or is otherwise unenforceable, such provision shall be deemed null and void only to the extent of such conflict or unenforceability, and shall be deemed separate from, and shall not invalidate, any other provision of this Agreement.
- XI. If Requesting Organization is a Qualified Entity (QE), some of the provisions contained within the DUA may not apply. In these situations, the Statewide Health Information Network for New York (SHIN-NY) regulations will apply. For QEs, MCD may only be used for treatment, quality improvement, to reduce medically adverse events, and to reduce costs through care coordination as authorized by 18 NYCRR 504.9. All QEs must submit proof of Qualified Entity Certification when returning the DUA form to DOH.
- XII. Confidentiality Statement
 - A. The Requestor has requested the data outlined in Section 3 ("the data") to enable its Office of Evaluation, Research and Policy unit to provide analysis and advice for and directly to the Commissioner of DSS, the Administrators of HRA and Department of Homeless Services (DHS), various deputy commissioners, and the heads of HRA and DHS program areas. OER uses administrative data and other resources to provide analysis of HRA and DHS programs and policies to inform decisions and strategic planning at multiple levels throughout the agencies. OER would use confidential Medicaid data in the MDW solely for the purpose of answering specific research questions posed

by internal DSS/HRA/DHS policymakers per "Sponsorship" and 17-088H for periods (dates): upon DUA approval and until December 31, 2021.

- B. Section 1902(a)(7) of the federal Social Security Act and Section 369(4) of the Social Services Law require that MCD be treated as confidential and used or disclosed only for purposes directly connected with the administration of the Medical Assistance program.
- C. The Requestor certifies to DOH that the Requestor, its officers, employees, agents or subcontractors will adhere to these Medicaid confidentiality standards and provisions of the legal authority cited by Requestor in the Purpose section. The Requestor will provide the following controls to ensure confidentiality of the MCD:
 - 1. The MCD may only be used for the purpose listed in this Agreement.
 - 2. Only listed Requestor staff that requires access to MCD to perform functions listed in this Agreement may be given access to the data. Such staff will be instructed by the Requestor in the confidential nature of the data and its proper handling.
 - 3. The MCD will be stored in locked storage receptacles for physical media or encrypted when in electronic format when the data are not under direct and immediate control of an authorized Requestor staff member engaged in work under this Agreement.
 - 4. The MCD, including any copies made by the Requestor, will be returned to DOH by the Requestor upon completion of the purpose outlined in the DUA, or with prior written DOH approval, the data may be destroyed by the Requestor after its use and a written confirmation provided by the Requestor to DOH of such destruction.
- XIII. Requestor, its contractors and subcontractors agree to sign the Federal Health Insurance Portability and Accountability Act/ Business Associate Agreement (HIPAA/BAA). Requestor agrees that all staff identified as having access to the MCD in any BAA, Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), contract or subcontracts must match the list provided to DOH. Requestor agrees that the statement of work to be done in the BAA, MOU, MOA, contract or subcontracts must match the purpose outlined in this DUA. Requestor agrees that the duration of the BAA, MOU, MOA, contract, or subcontracts must match the "start" and "end" date as stated in the DUA. Any description of destruction or return of MCD must match that as stated in the DUA.
- XIV. No individual claim-specific data in any form shall be combined or become a permanent part of another database or information sharing and retrieval system. Any use of individual recipient record data beyond this Agreement must have the written approval of DOH.
- XV. Requestor signs this Agreement as a condition for receipt of MCD to ensure maintenance of confidentiality and security of the data pursuant to the laws and provisions outlined within the DUA.

NYSDOH OHIP Data Use Agreement #:Click or tap here to enter text.

Date: Click here to enter a date.

5/8/18

Signature of Requestor:

Karen Lane

Requestor's Name (please print): Karen Lane

Requestor's Title (please print): Executive Deputy Commissioner, MICSA

Organization: HRA

Address: 4 World Trade Center, 150 Greenwich Street, New York, NY 10007

NOTARY

State of

New York

} ss.:

County of

New York

Subscribed and sworn to before me on this 8th day of May, 2018

Michael A. Porcello

Notarization

MICHAEL A PORCELLO
Notary Public, State of New York
No. 02POS043140
Qualified in Kings County
Commission Expires 5/8/2019

DOH Acceptance:

Date: Click here to enter a date.

5/10/2018

Signature of DOH Representative:

Muhammad amir

Signer's Name (please print): Click or tap here to enter text. Muhammad Amir

DUA Identification Number: Click or tap here to enter text. 17-088H

DUA Start Date: Click or tap here to enter text. 5/10/2018

Attachment A – HIPAA BUSINESS ASSOCIATE AGREEMENT

- I. As an entity receiving MCD from DOH under this Data Use Agreement (DUA), Requestor becomes a Business Associate of DOH and therefore agrees to the provisions of the BAA outlined below.
- II. Definitions. For purposes of this Agreement:
 - A. "Business Associate" shall mean: New York City Human Resources Administration/Department of Social Services
 - B. "Covered Program" shall mean: New York State Department of Health, Health Insurance Programs
 - C. Other terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and implementing regulations, including those at 45 CFR Parts 160 and 164.
- III. Obligations and Activities of Business Associate:
 - A. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.
 - B. Business Associate agrees to use the appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information (PHI) other than as provided for by this Agreement, and to comply with the security standards for the protection of electronic protected health information in 45 CFR Part 164, Subpart C. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
 - C. Business Associate agrees to report to Covered Program as soon as reasonably practicable any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware. Business Associate also agrees to report to Covered Program any Breach of unsecured PHI of which it becomes aware. Such report shall include, to the extent possible:
 1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 2. A description of the types of unsecured PHI that was involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information;
 3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 4. A description of what Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 5. Contact procedures for Covered Program to ask questions or learn additional information.
 - D. Business Associate agrees, in accordance with 45 CFR § 164.502(e)(1)(ii), to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.
 - E. Business Associate agrees to provide access, at the request of Covered Program, and in the time and manner designated by Covered Program, to PHI in a designated record set, to Covered Program in order for Covered Program to comply with 45 CFR § 164.524.

- F. Business Associate agrees to make any amendment(s) to PHI in a designated record set that Covered Program directs in order for Covered Program to comply with 45 CFR § 164.526.
 - G. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Program to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528; and Business Associate agrees to provide to Covered Program, in time and manner designated by Covered Program, information collected in accordance with this Agreement, to permit Covered Program to comply with 45 CFR § 164.528.
 - H. Business Associate agrees, to the extent the Business Associate is to carry out Covered Program's obligation under 45 CFR Part 164, Subpart E, to comply with the requirements of 45 CFR Part 164, Subpart E that apply to Covered Program in the performance of such obligation.
 - I. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Program available to Covered Program, or to the Secretary of the Federal Department of Health and Human Services (Secretary), in a time and manner designated by Covered Program or the Secretary, for purposes of the Secretary determining Covered Program's compliance with HIPAA, HITECH and 45 CFR Parts 160 and 164.
- IV. Permitted Uses and Disclosures by Business Associate
- A. Except as otherwise limited in this Agreement, Business Associate may only use or disclose PHI as necessary to perform functions, activities, or services for, or on behalf of, Covered Program as specified in this Agreement.
 - B. Business Associate may use PHI for the proper management and administration of Business Associate.
 - C. Business Associate may disclose PHI as required by law.
- V. Term and Termination
- A. This Agreement shall be effective for the term as specified in the contract between the Covered Entity and Business Associate, after which time all of the PHI provided by the Covered Program to Business Associate, or created or received by Business Associate on behalf of Covered Program, shall be destroyed or returned to Covered Program; provided that, if it is impracticable or not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in your contract.
 - B. Termination for Cause. Upon Covered Program's knowledge of a material breach by Business Associate, Covered Program may provide an opportunity for Business Associate to cure the breach and end the violation or may terminate this Agreement if Business Associate does not cure the breach and end the violation within the time specified by Covered Program, or Covered Program may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.
 - C. Effect of Termination.
 - 1. Except as provided in paragraph (C) (2) below, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Program, or created or received by Business Associate on behalf of Covered Program. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

2. In the event that returning or destroying the PHI is impracticable or not feasible, Business Associate shall provide to Covered Program notification of the conditions that prevented the return or destruction of the PHI. Upon mutual agreement of Business Associate and Covered Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction impracticable or not feasible, for so long as Business Associate maintains such PHI.

VI. Violations

- A. Any violation of this Agreement may cause irreparable harm to the Covered Program. Therefore, the Covered Program may seek any legal remedy, including an injunction or specific performance for such harm, without bond, security or necessity of demonstrating actual damages.
- B. Business Associate shall indemnify and hold the Covered Program harmless against all claims and costs resulting from acts/omissions of Business Associate in connection with Business Associate's obligations under this Agreement. Business Associate shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and hold harmless the Covered Program from suits, actions, damages and costs, of every name and description relating to breach notification required by 45 CFR Part 164 Subpart D, or State Technology Law § 208, caused by any intentional act or negligence of Business Associate, its agents, employees, partners or subcontractors, without limitation.

VII. Miscellaneous

- A. Regulatory References. A reference in this Agreement to a section in the Code of Federal Regulations means the section as in effect or as amended, and for which compliance is required.
- B. Amendment. Business Associate and Covered Program agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Program to comply with the requirements of HIPAA, HITECH and 45 CFR Parts 160 and 164.
- C. Survival. The respective rights and obligations of Business Associate under (IV) (C) of this Agreement shall survive the termination of this Agreement.
- D. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Program to comply with HIPAA, HITECH and 45 CFR Parts 160 and 164.
- E. HIV/AIDS. If HIV/AIDS information is to be disclosed under this Agreement, Business Associate acknowledges that it has been informed of the confidentiality requirements of Public Health Law Article 27-F.
- F. Alcohol and Substance Abuse. If Alcohol and Substance Abuse information is to be disclosed under this Agreement, Business Associate acknowledges that it has been informed of the confidentiality requirements of 42 CFR Part 2.

Business Associate (Subcontractor):

Name: Karen Lane

Entity: New York City Human Resources Administration

NYSDOH OHIP Data Use Agreement #:Click or tap here to enter text.

Signature: Karen Lane

Date: Click or tap to enter a date. 5/8/18

Covered Entity

Name: Muhammad Amir

Entity: NYS DOH Office of Health Insurance Programs

Signature: Muhammad amir

Date: 5/10/2018

Return to:
Security and Privacy Bureau
Medicaid Data Warehouse
Division of Systems
New York State Department of Health
Office of Health Insurance Programs
(518) 649-4397

Mailing address:
NYSDOH - MISCNY
ESP P1-11S Dock J
Albany NY 12237
medicaid.data.exchange@health.ny.gov

DEAA Template Names

[illegible]

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") effective as of January 26, 2018, is entered into by and between the New York City Department of Social Services ("DSS") / Human Resources Administration's ("HRA") Medical Insurance and Community Services Administration ("MICA") and Home Care Services Program/Managed Long Term Care ("HCSP" and "MLTC") (collectively known herein as "Covered Entity") and the following DSS and HRA program areas: Office of Legal Affairs ("OLA"); Office of Program Planning and Financial Management ("OPPFM") (which includes the Finance Office ("Finance"), the Office of Evaluation and Research ("OER"), and the office of Planning and Performance Management ("OPPM")); Office of External Affairs ("External Affairs") (which includes the Office of Citywide Health Insurance Access ("OCHIA") and the Office of Constituent Services ("OCS")); Office of Program Accountability ("OPA") (which includes the Investigation Revenue and Enforcement Administration ("IREA"), the Office of Audit and Quality Assurance ("OAQA"), the Special Investigation Division ("SID"), the Office of Program Accountability Support (OPAS), and the Office of Compliance and Contract Monitoring ("OCCM")); Customized Assistance Services ("CAS"); Information Technology Services ("ITS"); and the Public Engagement Unit ("PEU") (collectively herein known as the HRA "Business Associates") to comply with 45 C.F.R. §164.502(e) and §164.504(e), the regulations that govern protected health information ("PHI").

WHEREAS, the Covered Entity is comprised of the HRA programs that administer the public health plan, the Medicaid Program;

WHEREAS, the Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 (HIPAA) and its implementing regulations (45 CFR Parts 160, 162, and 164, subparts A, C, and E) (the "Privacy Rule") and 42 U.S.C. Section 1302d, et. seq., establish specific requirements related to the security and confidentiality of certain individually identifiable health information (defined in Section I (k) below as "Protected Health Information," or "PHI") and set forth the responsibilities and obligations of business associates to protect PHI; and

WHEREAS, the Health Information Technology for Economic and Clinical Health Act (HITECH), Public Law No. 111-5, 42 U.S.C. §§300jj *et seq.* and U.S.C. §17932 *et seq.* enacted as Title XIII of the American Recovery and Reinvestment Act ("ARRA") (Public Law 111-05), amends and extends certain provisions of HIPAA, making the HIPAA privacy and security regulations applicable to business associates;

WHEREAS, business associates are subject to the HIPAA Security Rule and must implement physical, administrative, technical safeguards to protect confidential electronic health records ("EHR");

WHEREAS, each Business Associate that is a party to this Agreement has been designated as such because in carrying out its responsibilities, functions and obligations under applicable law and in accordance with HRA policies and procedures it is authorized to create, receive, maintain, transmit, access, use and/or disclose PHI on behalf of MICA and HCSP/MLTC, the HIPAA Covered Entity; and

WHEREAS, HIPAA, Public Law No. 104-191, and the regulations promulgated thereunder, as the law and regulations may be amended, requires that Covered Entities and their Business Associates enter into a business associate agreement to provide satisfactory assurances that a Business Associate will appropriately safeguard PHI that it creates, receives, maintains, transmits, accesses, uses and/or discloses on behalf of a Covered Entity; and

WHEREAS, Business Associates may use or disclose PHI in accordance with HITECH (42 U.S.C. §300jj, §17931) and business associate agreements must include privacy provisions as mandated in HITECH (42 U.S.C. §17943); and

WHEREAS, HIPAA regulations provide that if a Covered Entity and its Business Associates are both governmental entities, a Covered Entity may comply with HIPAA by entering into a memorandum of understanding with its Business Associates that contains terms that accomplish the objectives of a business associate contract (see 45 CFR §164.504(e)(3)(i)(A)); and

WHEREAS, amendments to the HIPAA regulations published on January 25, 2013 (See 78 FR 5566) necessitate that the Parties enter into this Agreement for the purpose of each Business Associate providing satisfactory assurances to the Covered Entity that each Business Associate will appropriately safeguard the PHI of the Covered Entity by implementing appropriate physical, administrative and technical protections in accordance with the amended HIPAA regulations; and

WHEREAS, HRA's MICSA and HRA's HCSP/MLTC both comprise the Covered Entity because each assists in the administration of the State Medicaid plan, and HRA constitutes a HIPAA Hybrid Entity (as such term is defined in 45 CFR §164.103) because HRA's business activities include both covered and non-covered functions under HIPAA; and

WHEREAS, the parties hereto previously entered into a business associate agreement for the purpose of providing satisfactory assurances to the Covered Entity that each designated Business Associate will appropriately safeguard PHI disclosed by the Covered Entity; and

WHEREAS, HRA has undergone internal reorganization, and the parties seek to enter into this Agreement as a successor to the prior business associate agreement, upon the same terms therein, identifying the new parties comprising the HRA Business Associates.

NOW THEREFORE, the parties do hereby agree as follows:

I. DEFINITIONS

Except as otherwise defined herein, any and all terms used in this Business Associate Agreement shall have the same meaning as those terms in the HIPAA Rules, HITECH and as defined below:

(a) **"Breach"** shall have the same meaning as the term "breach" in 45 CFR §164.402 and 42 U.S.C. §17921.

(b) **"Business Associate"** shall have the same meaning as the term "Business Associate" in 45 CFR §160.103, and for this Agreement shall be the HRA Program area that creates, receives,

maintains, transmits, or accesses PHI on behalf of Covered Entity. As used in this Agreement, the term "Business Associates" shall further refer to the group comprised of OLA, OPPFM, External Affairs, OPA, CAS, ITS, and PEU, each individually a "Business Associate."

(c) **"Covered Entity"** shall have the same meaning as the term "covered entity" in 45 CFR §160.103, and for this Agreement shall be MICA, and the HCSP/MLTC, which are parties to the Agreement and are collectively designated as the HIPAA covered entity as it assists the State of New York in administering the Medicaid Program.

(d) **"Designated Record Set"** shall have the same meaning as the term "designated record set" in 45 CFR §164.501.

(e) **"Electronic Health Record"** shall mean an "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." 42 U.S.C. §17921.

(f) **"Electronic Protected Health Information" or "Electronic PHI"** shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103, except that Electronic PHI shall be limited to the information created, received, maintained, transmitted, or accessed by Business Associate or its Subcontractors or agents on behalf of Covered Entity.

(g) **"Health Care Component"** shall have the same meaning as the term "health care component" in 45 CFR §164.103.

(h) **"HIPAA"** shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191, and the regulations promulgated thereunder, as the law and regulations may be amended.

(i) **"HIPAA Rules"** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, as they may be amended.

(j) **"Individual"** shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

(k) **"Protected Health Information" or "PHI"** shall have the same meaning as the term "protected health information" in 45 CFR §160.103, except that PHI shall be limited to the information created, received, maintained, transmitted, or accessed by a Business Associate or its Subcontractors or agents on behalf of Covered Entity.

(l) **"Required by Law"** shall have the same meaning as the term "required by law" in 45 CFR §164.103.

(m) **"Secretary"** shall mean the Secretary of the United States Department of Health and Human Services or their designee.

(n) **"Security Incident"** shall have the same meaning as the term "security incident" in 45 CFR §164.304.

(o) **“Subcontractor”** shall have the same meaning as the term “subcontractor” in 45 CFR §160.103, and for this Agreement shall be a subcontractor of Business Associate.

(p) **“Unsecured Protected Health Information”** or **“Unsecured PHI”** shall have the same meaning as the term “unsecured protected health information” in 45 CFR §164.402. Unsecured PHI includes any PHI that is transmitted in any form that is rendered to be usable, readable or decipherable to unauthorized individuals.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) **Application.** This Agreement shall supersede all agreements pursuant to HIPAA entered into by and between any of the Parties prior to the Effective Date. This Agreement applies to the Health Care Components of the Parties and shall not apply to the non-covered functions of those programs.

(b) **Permitted or Required Uses.** Each Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as required by law. Business Associates shall not use or disclose PHI in any manner that would constitute a violation of HIPAA or HITECH.

Each Business Associate acknowledges that this Agreement does not in any manner grant any Business Associate any greater rights than the Covered Entity enjoys, nor shall it be deemed to permit or authorize any Business Associate to use or further disclose PHI in a manner that would otherwise violate the requirements of HITECH and/or HIPAA if conducted by the Covered Entity.

Each Business Associate agrees that it is not permitted to use or disclose PHI without an authorization or consent, unless: (1) such a use and/or disclosure absent consent is in accordance with 45 C.F.R. §164.506, §164.510, §164.512, §164.514(e), §164.514(f), §164.514(g) and such use and/or disclosure is authorized in writing by the DSS Chief Privacy Officer and/or General Counsel; or (2) such a use and/or disclosure is otherwise permitted or required by agreement or Required by Law; except that each Business Associate may use PHI received in its capacity as a business associate to the Covered Entity, if necessary for the proper management and administration of the Business Associate’s legitimate work-related activities.

If any Business Associate chooses to use or disclose any PHI for any purpose that is not directly connected with the administration of the Medicaid Program, in accordance with New York State Social Services Law §§136 and 369(4), 42 USC §1320(d), 42 C.F.R. §431.300 or for any other purpose not authorized by this Agreement, absent a court order, the Business Associate must make a written request to the Executive Deputy Commissioner of MICSA, the Deputy Commissioner of HCSP, and the DSS Chief Privacy Officer in the Office of Legal Affairs, describing the purpose for the disclosure, the type of PHI to be disclosed, the entity to whom the data will be disclosed and the source of the data.

The Parties agree that any Party hereto may only disclose, transmit, or otherwise grant access to PHI pursuant to this Agreement if the Covered Entity or Business Associate has such PHI in its possession. This Agreement shall not be construed to permit any Party to disclose, transmit, or

otherwise grant access to any PHI to which the Party itself merely has access (i.e. a State-owned database containing PHI that a Party regularly accesses in performance of its functions, but that the Party does not own, possess or maintain).

(c) **Appropriate Safeguards.** Each Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement, and with respect to Electronic PHI to comply with Subpart C of 45 CFR Part 164 (45 CFR §164.302 et seq.). The safeguards shall include administrative, procedural, physical, electronic and technical measures that reasonably and appropriately protect the confidentiality, security, integrity and availability of the PHI that the Business Associate receives, creates, maintains or transmits on behalf of the Covered Entity as required by 45 CFR § Part 164. Each Business Associate shall also implement such safeguards to prevent the misuse of PHI other than as provided by this Agreement. The parties recognize that Section 13401 of the HITECH Act makes certain provisions of HIPAA relating to the security of PHI directly applicable to Business Associates. Business Associates shall use appropriate safeguards to ensure the security and confidentiality of the PHI in its transmission. Business Associates shall establish and maintain comprehensive written policies (or, collectively, a single policy that applies to each Business Associate) regarding such safeguards. It is the responsibility of the Business Associate to inform and train staff that has direct access to PHI of such policies.

(d) **Mitigation.** Each Business Associate agrees to promptly correct and mitigate, to the extent practicable, any harmful effects of which that Business Associate becomes aware that have resulted from any unauthorized acquisition, access, use or disclosure of PHI by the Business Associate, its contractors, subcontractors or agents.

(e) **Reporting Unauthorized Use or Disclosure.** The parties recognize that Section 13402 of the HITECH Act requires business associates to notify the Covered Entity in the event of i) any unauthorized disclosure of PHI; ii) breach of security relating to unsecured PHI; and/or iii) any suspected or actual data security breach relating to unsecured PHI of which the Business Associate becomes aware. Each Business Associate agrees to report to the HRA General Counsel and the DSS Chief Privacy Officer, upon discovery of any use or disclosure of PHI not provided for or authorized by this Agreement. For any suspected or actual data security Breach, the Business Associate shall notify the Covered Entity in writing within five (5) business days of having been made aware of such unauthorized acquisition, access, use or disclosure of PHI by any party, including the Business Associate.

Such notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the breach. The Business Associate shall provide the Covered Entity and the DSS Chief Privacy Officer with other information as it becomes available, including (1) a brief description of what happened and when, (2) the names of the parties involved, (3) a description of the types of PHI compromised, (4) steps taken to mitigate the harm, (5) recommendations to the affected individuals regarding steps that should be taken to protect themselves from potential harm resulting from the breach; and (6) a brief description of what the Business Associate is doing to investigate the breach, mitigate harm to individuals and protect against any future breaches.

Each Business Associate agrees to fully cooperate with any investigation conducted by the Covered Entity or its designated agents of any such unauthorized acquisition, access, use or disclosure.

(f) Breach Notification Under HIPAA Rules.

(1) Each Business Associate agrees to comply with the requirements of Subpart D of 45 CFR Part 164 (45 CFR §164.400 et seq.), including but not limited to the requirement that, following the discovery of any Breach of Unsecured PHI, the Business Associate shall, without unreasonable delay, and in no event later than (5) days after discovery of any Breach of Unsecured PHI, provide notification as specified in section II (e) above.

In the event of a Breach or suspected Breach of Unsecured PHI, each Business Associate shall provide the Covered Entity and the DSS Chief Privacy Officer and HRA General Counsel with an explanation in writing of the basis for its determination that an unauthorized disclosure of unsecured PHI has occurred. The OLA Office of Data Privacy will conduct a risk assessment in accordance with 45 CFR §164.402 (see paragraph (2) in definition of "Breach"), to determine whether a Breach of Unsecured PHI has occurred. The Business Associate shall provide the DSS Chief Privacy Officer with any documentation requested by OLA to perform its investigation and assessment.

(2) If the DSS Chief Privacy Officer determines that an unauthorized acquisition, access, use or disclosure of PHI has occurred and has been reported to the Covered Entity as required by Section II(d) or Section IV(c), but has been determined not to constitute a Breach of Unsecured PHI, the DSS Chief Privacy Officer shall provide the Covered Entity with an explanation in writing of the basis for such determination and any risk assessment conducted under 45 CFR §164.402 (see paragraph (2) in definition of "Breach"), and all documentation in support of such determination. Such explanation in writing shall be provided without unreasonable delay, and in no event later than sixty (60) days after the discovery of the unauthorized acquisition, access, use or disclosure of PHI.

(g) Contractors, Subcontractors and Agents. In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), as applicable, each Business Associate agrees to ensure that all of its contractors, subcontractors and agents that create, receive, maintain, transmit, or access PHI on behalf of the Business Associate, agree in writing to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. A Business Associate is not in compliance with this Agreement if the Business Associate knew of a pattern of activity or practice of a contractor, subcontractor or agent that constituted a material breach or violation of the contractor's, subcontractor's or agent's obligations under its subcontract, unless each Business Associate took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the contract or subcontract, if feasible.

(h) Access by Individual. Each Business Associate shall maintain a designated record set, as defined by HIPAA, for each individual client for which it has PHI. In accordance with an individual's right to access to their own PHI under HIPAA, each Business Associate agrees to provide access to PHI in a designated record set, at the request of Covered Entity, to an

individual or individual's representative to satisfy Covered Entity's obligations under 45 CFR §164.524. Each Business Associate shall make all PHI in that designated record set available to the individual to whom that information pertains, or such individual's representative.

(i) **Amendment to PHI.** Each Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of the Covered Entity or an individual, and in the reasonable time and manner designated by the Covered Entity, and to take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR §164.526, provided that the Business Associate has PHI in a Designated Record Set.

(j) **Request for an Accounting.** Each Business Associate agrees to document disclosures of individually identifiable PHI, and information related to such disclosures, as would be required for the Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528. Each Business Associate agrees to make available to Covered Entity or an individual, in the reasonable time and manner designated by the Covered Entity, information collected pursuant to this Section II(j) in order to provide an accounting of disclosures as necessary to satisfy the Covered Entity's obligations under 45 CFR §164.528.

(k) **Additional Restrictions on PHI.** If the Covered Entity notifies a Business Associate that it agreed to be bound by additional restrictions on the uses or disclosures of certain PHI pursuant to the HIPAA Rules, each Business Associate agrees to be bound by such additional restrictions and shall not disclose such PHI in violation of such additional restrictions.

(l) **Carrying Out Covered Entity Obligation(s).** To the extent that a Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164 (45 CFR §164.500 et seq.), the Business Associate shall comply with the requirements of such Subpart E that apply to the Covered Entity in the performance of such obligation(s).

(m) **Access by Secretary to Determine Compliance.** Each Business Associate agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI created, received, maintained, transmitted, or accessed by the Business Associate on behalf of the Covered Entity, available to the Covered Entity and to the United States Department of Health and Human Services ("DHHS") Secretary at the direction of the Office of Legal Affairs, in the reasonable time and manner designated by the Covered Entity, or in the time and manner designated by the Secretary, as applicable, for purposes of determining compliance with the HIPAA Rules. A Business Associate shall immediately notify the Covered Entity upon receipt of any request by the Secretary for access and of all materials to be disclosed pursuant to such request.

(n) **Records; Covered Entity Access.** Each Business Associate shall maintain such records of PHI received from, or created or received on behalf of, the Covered Entity and shall document subsequent uses and disclosures of such information by the Business Associate as may be deemed necessary and appropriate in the sole discretion of the Covered Entity from the date of execution of the Agreement until the Agreement is terminated in writing. Each Business Associate shall provide the Covered Entity with reasonable access to examine and copy such records and documents of the Business Associate during regular business hours. Each Business

Associate agrees to fully cooperate in good faith with and to assist the Covered Entity in complying with the requirements of HIPAA and any investigation of the Covered Entity regarding compliance with HIPAA conducted by the DHHS Office of Civil Rights, or any other administrative or judicial body with jurisdiction.

III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

(a) **Use and Disclosure for Performance.** Except as otherwise provided in this Agreement, each Business Associate may only use or disclose PHI as necessary to perform services, functions, activities, and/or duties for, or on behalf of, the Covered Entity as specified in this Agreement, or as necessary to perform its duties under this Agreement, or as Required by Law, provided that such use or disclosure would not violate the HIPAA Rules if done by the Covered Entity. Disclosure of PHI to third parties shall only be permissible after consulting with the DSS Chief Privacy Officer and after obtaining approval for the re-disclosure from HRA's Office of Legal Affairs. The third parties shall provide written assurances of their confidential handling of such PHI, which shall include adherence to the same restrictions and conditions on use and disclosure as apply to Business Associates herein.

(b) **Minimum Necessary Use and Disclosure.** In accordance with the HIPAA Rules, when using or disclosing PHI, or when requesting PHI from the Covered Entity or another covered entity or business associate, each Business Associate agrees to make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

(c) **Disclosure for Management, Administration and Legal Responsibilities.** Each Business Associate may disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that the disclosure is required by law and the recipient of PHI has agreed to notify the Business Associate of any instances of which it is aware or becomes aware that the confidentiality of the information has been disclosed without authorization. To the extent permitted by applicable law, prior to disclosing PHI as Required by Law to a law enforcement, regulatory, administrative, or oversight agency, or in response to a subpoena, court order, civil investigative demand, or other compulsory document or lawful process, each Business Associate shall notify the Covered Entity and HRA's Office of Legal Affairs of such pending disclosure and provide reasonable time for the Covered Entity to oppose such disclosure, should the Covered Entity deem such opposition necessary; provided, however, that if the Covered Entity does not respond to the Business Associate regarding such opposition prior to the date on which such disclosure must be timely made, the Business Associate may, in its own discretion, disclose PHI as Required by Law or such lawful process.

(d) **De-identified PHI.** Each Business Associate agrees that it will obtain the prior approval of the Covered Entity and the DSS Chief Privacy Officer before de-identifying PHI in accordance with 45 CFR §164.514(a)-(c) and utilizing such de-identified PHI.

(e) **Use of PHI or De-identified PHI for Research Purposes.** Each Business Associate agrees that it will obtain the prior approval of the Covered Entity and HRA's Office of Legal Affairs for the use or disclosure of PHI or de-identified PHI for research purposes.

(f) Use of PHI for Research Purposes. Absent individual consent, research studies conducted by Business Associates that use PHI must meet the criteria of being directly connected with the administration of medical assistance. 42 U.S.C. §1396a (a)(7); NY SSL §369(4). The federal regulations that govern the use and disclosure of Medicaid data define Medicaid program administration to include (A) establishing eligibility; (B) determining the amount of Medical Assistance; (C) providing services for beneficiaries; and (D) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan. 42 CFR §431.302.

Absent individual consent, HIPAA allows the use and disclosure of Medicaid data for reviews preparatory to research. When conducting research using PHI absent individual consent, the Business Associate shall provide the Covered Entity with representations, either in writing or orally, that the use or disclosure of the PHI is sought solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any PHI from the Covered Entity, and representation that PHI for which access is sought is necessary for the research purpose. 45 CFR 164.512(i)(1)(ii).

IV. SECURITY REQUIREMENTS

(a) Safeguards to Protect Electronic PHI. All Business Associates agree to comply with the applicable requirements of Subpart C of 45 CFR Part 164 (45 CFR §164.302 et seq.), which include but are not limited to, implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that the Business Associate creates, receives, maintains, transmits, or accesses on behalf of the Covered Entity. The Business Associates shall not use or disclose PHI for any purpose other than for the purposes for which access to such PHI was authorized by the Covered Entity and HRA's Office of Legal Affairs.

(b) Contractors, Subcontractors and Agents. In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), as applicable, each Business Associate agrees to ensure that all of its contractors, subcontractors and agents that create, receive, maintain, transmit, or access Electronic PHI on behalf of the Business Associate agree in writing to comply with the applicable requirements of Subpart C of 45 CFR Part 164 (45 CFR §164.302 et seq.), which include but are not limited to, implementing reasonable and appropriate safeguards to protect such information.

V. COMPLIANCE WITH CERTAIN FEDERAL AND NEW YORK STATE LAWS

(a) Confidentiality Under New York Law. Each Business Associate agrees to comply with all applicable New York State laws and any federal laws and regulations promulgated thereunder governing the confidentiality of PHI created, received, maintained, transmitted, or accessed by the Business Associate, its subcontractors or agents on behalf of the Covered Entity, including but not limited to the following provisions, as applicable: HIPAA, Public Law 104-191; HITECH, Public Law 111-5, 42 U.S.C. §300jj et seq. and 42 U.S.C. §17932; Federal Social Security Act, 42 U.S.C. §1396a(a)(7) and its implementing federal regulation 42 C.F.R. §431.300, New York State Social Services Law §§136, 367-b, and 369(4) 372, 422, and 473-e, its implementing state regulations, 18 N.Y.C.R.R. Parts 357, 360-8, 403.9, 457.16; New York

Public Health Law, §18 (Access to Patient Information) and Article 27-F (HIV and AIDS Related Information); New York Mental Hygiene Law §§22.05 and 33.13; New York Civil Rights Law §79-l; New York General Business Law §399-ddd (Confidentiality of Social Security Account Numbers), §399-h and §899-aa; NYS Public Officers Law §96a and chapter 5 of Title 10 of the Official Compilation of Codes, Rules, and Regulations of the State of New York.

(b) **Breach Notification Under New York Law.** Pursuant to Title 10 of the Administrative Code of the City of New York ("NYC Administrative Code"), §10-501 and all other applicable federal, state, and local laws, and in conformity with Section II(d) and Section IV(c) of this Agreement, each Business Associate shall, within five (5) business days of discovery thereof, notify the Covered Entity of any "breach of the security," as defined in NYC Administrative Code §10-501(b), that involves PHI containing individuals' "personal identifying information," as defined in NYC Administrative Code §10-501(a), that was, or was reasonably believed to be, acquired from the Business Associate, its subcontractors or agents by a person without valid authorization.

(c) **Requirements of Section 11 of New York State Department of Health ("NYSDOH") Office of Health Insurance Programs ("OHIP") Data Use Agreement.**

(1) Medicaid Confidential Data/Protected Health Information ("MCD/PHI") provided to or accessed by the Covered Entity or Business Associates from the NYSDOH Medicaid Data Warehouse ("MDW") or other recognized NYSDOH data source includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

(2) Business Associates must comply with the following state and federal laws and regulations:

- (i) Section 367-b(4) of the NY Social Services Law
- (ii) New York State Social Services Law Section 369(4)
- (iii) Article 27-F of the New York Public Health Law and 18 NYCRR 360-8.1
- (iv) Social Security Act, 42 USC 1396a(a)(7)
- (v) Federal regulations at 42 CFR 431.302 and 42 CFR Part 2
- (vi) HIPAA and HITECH, at 45 CFR Parts 160 and 164
- (vii) NYS Mental Hygiene Law Section 33.13.

(3) Please note that MCD/PHI released to a Business Associate may contain AIDS/HIV related confidential information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5)(a), the following notice is provided to the Business Associates: "This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any

further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure.”

(4) **Alcohol and Substance Abuse Related Confidentiality Restrictions:** Alcohol and substance abuse information is confidential pursuant to 42 CFR Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

(5) **Business Associates agree that each Business Associate and any agent, including a subcontractor, to whom Business Associate provides MCD/PHI, agrees to the same restrictions and conditions that apply throughout this Agreement.** Further, Business Associates agree to state in any such agreement, contract or document that the party to whom Business Associate is providing the MCD/PHI may not further disclose it without the prior written approval of the New York State Department of Health. Business Associates agree to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that a Business Associate enters into that involves MCD/PHI.

VI. OBLIGATIONS OF COVERED ENTITY

(a) **Notify of Limitation(s) in Privacy Notice.** The Covered Entity shall notify each Business Associate of any limitation(s) in the notice of privacy practices utilized by the Covered Entity under 45 CFR §164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of PHI.

(b) **Notify of Changes in Individual's Permission.** The Covered Entity shall notify each Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

(c) **Notify of Restriction on Use or Disclosure.** The Covered Entity shall notify each Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

(d) **Impermissible Request by Covered Entity.** The Covered Entity shall not request any Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or the HITECH ACT if performed by the Covered Entity.

VII. TERM AND TERMINATION

(a) **Term.** This Agreement shall be effective from the date of execution of the Agreement through December 31, 2021, unless terminated in writing by the parties or as otherwise provided herein.

(b) **Termination for Violation of Material Term.** Each Business Associate acknowledges and agrees that the Covered Entity shall have the right to immediately terminate this Agreement with respect to any individual Business Associate in the event the Business Associate fails to comply with HIPAA requirements concerning PHI, or any material term of this Agreement, as determined by the Covered Entity in its sole discretion. In the event that the Covered Entity reasonably believes that a Business Associate may have violated a material term of this Agreement, the Covered Entity and HRA's Office of Legal Affairs shall have the right to investigate such violation, and the Business Associate shall fully cooperate with any such investigation. Alternatively, the Covered Entity may provide written notice to a Business Associate of the existence of a violation of a material term of this Agreement, and afford the Business Associate an opportunity to cure such violation to the satisfaction of the Covered Entity within thirty (30) days of receiving notice of the violation or such other period of time as the parties may agree to. Termination pursuant to this Section VII(b) shall be effectuated by a written notice to a Business Associate that specifies the violation upon which the termination is based and the effective date of the termination. In the event of such termination, this Agreement shall remain in effect with respect to the non-breaching Business Associates.

(c) **Effect of Termination.**

(1) Except as provided in paragraph (2) of this Section VII(c), upon termination or expiration of the Agreement, the Business Associate, shall return to the Covered Entity or, if agreed to by the Covered Entity, destroy any PHI received from the Covered Entity, that the Business Associate created or maintained in any form, on behalf of the Covered Entity, and ensure that its contractors, subcontractors and agents return or destroy, in a manner consistent with HRA's policies and procedures for record disposal, all PHI received from the Covered Entity, or created, maintained, received, or accessed by or on behalf of the Business Associate or the Covered Entity, that the Business Associate, its contractors, subcontractors or agents still maintain in any form. Each Business Associate shall not retain, and shall ensure that its contractors, subcontractors and agents not retain, copies of the PHI.

(2) Each Business Associate shall retain only that PHI which is necessary for the Business Associate to continue its proper management and administration or to carry out its legal responsibilities.

(3) Each Business Associate shall continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as the Business Associate retains the PHI.

(d) **Non-exclusive Provisions.** The termination provisions of this Section VII are in addition to, and not in lieu of, the termination provisions provided elsewhere in the Agreement and any other rights and remedies of the Covered Entity that are provided by law or by such Agreement.

VIII. MISCELLANEOUS

(a) **Agency.** For purposes of this Agreement, it is the understanding and intention of the parties that each Business Associate is acting as an agent of the Covered Entity.

(b) **References to Law and Rules.** A reference in this Agreement to any section of law or rules (including but not limited to the HIPAA Rules), means the section of law or rules as in effect or as amended.

(c) **Amendment.** Each Business Associate agrees that this Agreement may be amended from time to time upon written notice from the Covered Entity to the Business Associate as to the revisions required to make this Agreement consistent with applicable law and rules. This Agreement may also be amended to add or remove Business Associates.

(d) **Survival.** The respective rights and obligations of each Business Associate and the Covered Entity under the provisions of this Agreement shall survive the expiration or termination Agreement.

(e) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity and a Business Associate to comply with the HIPAA Rules and the applicable State laws cited in Section V of this Agreement.

(f) **Successors and Assigns.** A successor agency or assign of any Party to this Agreement shall be subject to all of the terms and conditions of this Agreement applicable to such Party.

(g) **No Third Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.

(h) **Counterparts.** This Agreement may be executed in any number of counterparts, each of which when so executed will be deemed to be an original and all of which when taken together will constitute one Agreement.

(i) **Entire Agreement.** This Agreement constitutes the entire agreement and supersedes all prior agreements and understandings, both written and oral, among the Parties with respect to the subject matter of this Agreement.

-NO FURTHER TEXT ON THIS PAGE-

IN WITNESS WHEREOF, the Parties affirm their understanding of the terms herein by executing this Agreement on the dates appearing below their respective signatures.

Medical Insurance and Community Services Administration:

Signature: Karen Lane

Printed Name: Karen Lane

Title: Executive Deputy Commissioner, MICSA

Date: 1/26/18

Home Care Services Program:

Signature: [Signature]

Printed Name: Arnold Ng

Title: Deputy Commissioner Home Care Services Program

Date: 1/26/2018

Office of Legal Affairs:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Program Planning and Financial Management:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

IN WITNESS WHEREOF, the Parties affirm their understanding of the terms herein by executing this Agreement on the dates appearing below their respective signatures.

Medical Insurance and Community Services Administration:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Home Care Services Program:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Legal Affairs:

Signature: *[Signature]*

Printed Name: Martha A. Galloway

Title: General Counsel

Date: 7/24/18

Office of Program Planning and Financial Management:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

IN WITNESS WHEREOF, the Parties affirm their understanding of the terms herein by executing this Agreement on the dates appearing below their respective signatures.

Medical Insurance and Community Services Administration:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Home Care Services Program:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Legal Affairs:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Program Planning and Financial Management:

Signature: EL

Printed Name: Ellen Levine

Title: Chief Program Planning & Financial Management

Date: 1/26/2018

Officer

External Affairs:

Signature: Maria Teresa Arce

Printed Name: MARIA TERESA ARCE

Title: CHIEF EXTERNAL AFFAIRS OFFICER

Date: 1/29/2018

Office of Program Accountability:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Customized Assistance Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Information Technology Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

B – Internal HRA Business Associate Agreement
FINAL - 1/23/18

External Affairs:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Program Accountability:

Signature: S. Ghartey

Printed Name: Saratu Ghartey

Title: Chief Prog Accountability Officer

Date: 1/30/2018

Customized Assistance Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Information Technology Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

B – Internal HRA Business Associate Agreement
FINAL - 1/23/18

External Affairs:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Program Accountability:

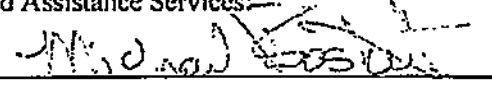
Signature: _____

Printed Name: _____

Title: _____

Date: _____

Customized Assistance Services:

Signature:  _____

Printed Name: Michael Bosket

Title: Deputy Commissioner

Date: 1/24/18

Information Technology Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

External Affairs:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Office of Program Accountability:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Customized Assistance Services:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Information Technology Services:

Signature:  _____

Printed Name: Richard Browne

Title: Chief Information Officer

Date: 1/25/2018

B – Internal HRA Business Associate Agreement
FINAL - 1/23/18

Public Engagement Unit:

Signature: 

Printed Name: ERIC Rotondi

Title: Deputy Director

Date: 1/26/2018