MEMORANDUM OF UNDERSTANDING AND BUSINESS ASSOCIATE AGREEMENT BETWEEN THE NEW YORK CITY DEPARTMENT OF FINANCE AND THE NEW YORK CITY HUMAN RESOURCES ADMINISTRATION

MEMORANDUM OF UNDERSTANDING ("MOU") made and entered into this 28th day of January, 2020, by and between THE NEW YORK CITY DEPARTMENT OF FINANCE ("DOF"), with its headquarters located at 1 Centre St, New York, NY 10007, and THE NEW YORK CITY DEPARTMENT OF SOCIAL SERVICES, acting by and through its HUMAN RESOURCES ADMINISTRATION ("HRA"), with its offices located at 150 Greenwich Street, New York, NY 10007.

WITNESSETH:

WHEREAS, DOF administers the tax and revenue laws of New York City fairly, efficiently and transparently to instill public confidence and encourage compliance while providing exceptional customer service; and

WHEREAS, HRA administers the Medicaid Surplus Program in New York City, through which eligible individuals have the option to pay their excess income to the local social services district in order to qualify for Medicaid ("Payments"); and

WHEREAS, DOF, as the manager of the City's cash flow and Citywide Payment Services, has agreed to provide an online homepage and gateway that is compliant with all City banking policies and applicable state laws, and card associations rules and regulations, to allow MA clients to make Payments directly to HRA online using a credit card; and

WHEREAS, to that end, it is necessary for HRA to electronically transfer to DOF on a daily basis electronic data identifying HRA's Medicaid Surplus Program clients who can make Payments ("MA Client Data"); and

WHEREAS, HRA is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA") with respect to its Medicaid operations, and the MA Client Data as herein defined constitutes protected health information ("PHI") subject to HIPAA's Privacy and Security Regulations (as set forth in 45 CFR Parts 160 and 164); and

WHEREAS, HRA has determined that the sharing of the MA Client Data with DOF is necessary for the aforementioned payment operations; and

WHEREAS, disclosure of PHI without patient consent is authorized for payment operations by the Privacy Regulations promulgated by the United States Department of Health and Human Services pursuant to HIPAA; and

WHEREAS, DOF's receipt of the Payments cannot be accomplished except with the use of identifiable PHI, and the PHI to be provided to DOF will be the minimum necessary for the payment operations sought to be accomplished; and

WHEREAS, by receiving the MA Client Data for the purposes stated herein, DOF is a business associate of HRA, and, accordingly, this MOU shall serve as the business associate agreement between the parties hereto, in compliance with HIPAA Privacy Regulations; and

WHEREAS, DOF and HRA now agree to engage in the daily transfer of MA Client Data, subject to the terms and conditions set forth of this MOU;

NOW, THEREFORE, the parties hereto agree as follows:

I. TERM

A. This MOU shall take effect as of the date first set forth above and remain in effect for as long as DOF continues to accept the Payments on behalf of HRA, unless the MOU is sooner terminated as provided herein.

II. TRANSFER, STORAGE, HANDLING, USE AND DISPOSAL OF MA CLIENT DATA

A. HRA shall transfer to DOF the following MA Client Data for MA clients who have made payments previously to HRA within a specified timeframe, which is the minimum necessary disclosure for DOF to perform its payment operations, on a daily basis via Secure File Transfer Protocol ("SFTP") and in a mutually agreed-upon format:

1. CIN Number
2. Client First Name
3. Client Last Name
4. Category Code of "MAPIP"
5. Last 4 digits of client's Social Security Number
6. Case Number

B. The homepage and gateway provided by DOF shall comply with all City banking policies and applicable state laws, and card associations rules and regulations, and shall enable clients to make Payments directly to HRA for the requested coverage dates. Clients will be able to search the portal by CIN and the last 4 digits of the client's Social Security Number.

C. DOF shall store the MA Client Data in a secure computer environment, separate from other data, for so long as it maintains such data. DOF shall ensure that the MA Client Data is encrypted in transmission. DOF shall also ensure that the MA Client Data is encrypted at rest by the end of the first quarter of 2020, when it completes upgrades to its server that will allow it to encrypt data at rest. If DOF cannot encrypt MA Client Data at rest by the end of the first quarter of 2020, , this

shall constitute a material breach and HRA shall have the right to terminate this MOU immediately for cause.

D. Access to the MA Client Data shall be limited to authorized DOF staff directly engaged in administering the Payments.

E. DOF shall report back to HRA on which clients have made Payments. The MA Client Data returned by DOF to HRA shall contain all of the data elements referenced in Article II.A above, as well as the following:

1. Payment amount for each client matched to the individual client; and
2. Date of Payment; and
3. Requested coverage dates.

E. DOF shall first obtain written HRA approval pursuant to this MOU should it wish to use the MA Client Data or Match Data for any purpose or in any manner other than as set forth herein.

F. DOF shall use the MA Client Data solely for the purpose of accepting the Payments as directed by HRA.

G. DISPOSAL OF DATA. At such time as DOF no longer requires use of any portion of the MA Client Data in its possession, DOF shall delete the MA Client Data and any other data or documentation that contains MA Client, in a manner that ensures that it cannot reasonably be retrieved. DOF shall periodically certify in writing, on an annual basis or other mutually agreeable frequency, that it is securely deleting MA Client Data no longer needed by DOF for the purpose set forth in this MOU.

H. HRA shall have the right to view, upon request and reasonable notice to DOF, and subject to DOF's approval, to DOF's storage, handling, use and disposal of the MA Client Data. DOF shall cooperate with any such request, including providing documentation of DOF's confidentiality, security and disposal procedures, if required, subject to DOF's requirements for confidentiality and tax secrecy as provided by law, rule, policy or agreement.

III. HIPAA BUSINESS ASSOCIATE PROVISIONS

A. Inasmuch as DOF's access to and use of the MA Client Data may render it a business associate pursuant to HIPAA, the parties hereby incorporate by reference the terms and conditions set forth in Attachment A hereto, which constitute a business associate agreement in conformance with HIPAA requirements. In case of any conflict between the terms of this MOU and these business associate provisions, the terms of the business associate provisions shall govern.

IV. LEGAL BASIS FOR DISCLOSURE

A. HRA may disclose the MA Client Data to DOF absent patient consent pursuant to 45 CFR 164.506(c)(1), which states that a covered entity may use or disclose protected health information for its own treatment, payment or health care operations.

V. EFFECT OF UNAUTHORIZED DISCLOSURE

A. The Parties agree to report any unauthorized disclosures of the other Party's confidential or protected data, not provided for by this MOU, of which they become aware. The Parties further agree to immediately report any data security incident of which they become aware, including a breach of unsecured protected data.

B. In the event of any unauthorized disclosure of data, the Party responsible for the unauthorized disclosure of data (Responsible Party) shall immediately commence an investigation to determine the scope of the disclosure and immediately inform the other Party (Affected Party) following discovery of such incident. The Responsible Party shall provide a written incident report, within forty-eight (48) hours after the incident is discovered, that details the circumstances surrounding the unauthorized disclosure and the names of the individuals affected by the unauthorized disclosure, if known. Such incident is considered discovered on the first day on which the Responsible Party knows of such incident.

C. In the event of a data breach, the Responsible Party is required to notify the affected individuals within a reasonable amount of time, but no later than sixty (60) calendar days after the discovery of the breach or earlier if so required by law, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. Notification shall be in a form and format prescribed by the Affected Party and shall meet the requirements of applicable local, state, and federal law. The Responsible Party shall be responsible for all costs associated with providing notification to all affected individuals when notification is required by law.

V. TERMINATION

A. Either party may terminate this MOU upon thirty (30) days prior written notice to the representative of the other party designated pursuant to Paragraph VI herein.

B. Upon termination of this MOU, DOF shall destroy any and all MA Client Data in its possession, and certify in a form satisfactory to HRA that such destruction has been completed in a manner satisfactory to HRA, and in accordance with the terms of this MOU.

VI. NOTICES

A. Any notice to be given pursuant to this MOU shall be in writing and shall be deemed to have been given when: (1) delivered in person, against receipt; (2) sent by certified mail, return receipt requested; (3) delivered by overnight or same-day courier service in a properly addressed envelope, with written confirmation; or (4) e-mailed or sent by facsimile transmission.

B. The parties hereby designate the following representatives for receipt of notice pursuant to this MOU, or such other representatives as they may designate in writing:

Notice to DOF:

Samuel Bufter
Deputy Director of Implementation and Technology Solutions
Citywide Payment Services and Standards,
NYC Department of Finance
59 Maiden Lane, 18th Floor
New York, NY 10038

Notice to HRA:

Harold Delaney
Deputy Commissioner of Fiscal Operations
NYC Department of Social Services
150 Greenwich Street, 34th Fl
New York, NY 10007

With a copy to:

NYC Department of Social Services
150 Greenwich Street, 38th Floor
New York, NY 10007
Attn: Chief Data Privacy Officer

VII. MERGER AND MODIFICATION

A. This MOU constitutes the entire agreement between the Parties, and merges into it all prior discussions, agreements or understandings, written or oral, between the parties.

B. This MOU may be extended, amended or otherwise modified in writing signed by authorized representatives of the parties. It may not be extended, amended or otherwise modified orally.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

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

THE NEW YORK CITY DEPARTMENT OF SOCIAL SERVICES

Signature

Name

Title

Date

THE NEW YORK CITY DEPARTMENT OF FINANCE

Signature

Peter S. Smith

Name

Asst Commr CPSS

Title

1/28/2020

Date

STATE OF NEW YORK)
:ss
COUNTY OF NEW YORK)

On this 11th day of 2020, before me personally came Vincent Pugh to me known and known to me to be NCCO of the HUMAN RESOURCES ADMINISTRATION of the CITY OF NEW YORK, the person described in and who executed the foregoing instrument, and she/he acknowledged to me that she/he executed the same for the purpose therein mentioned.

SHARON JAMES-LEONCE
Commissioner of Deeds
City of New York No. 2-13026
Certificate Filed in New York County
Commission Expires May 01, 2020

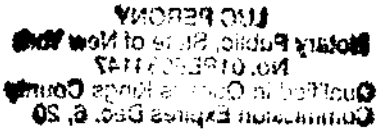
Sharon James-Leonce
Notary Public

On this 28th day of Jan 2020, before me personally came Peter S. Smith, to me known and known to me to be the Assistant Commissioner of CPSS, the person described in and who executed the foregoing instrument, and she/he acknowledged to me that she/he executed the same for the purpose therein mentioned.

Notary Public

LUC PERONY
Notary Public, State of New York
No. 01PE6034147
Qualified in Queens/Kings County
Commission Expires Dec. 6, 2021

ATTACHMENT A



Health Insurance Portability and Accountability Act

Business Associate Agreement

This Business Associate Agreement, Attachment A ("the Agreement") is effective as of the effective date of the MOU to which it is attached, by and between THE NEW YORK CITY DEPARTMENT OF SOCIAL SERVICES acting by and through its HUMAN RESOURCES ADMINISTRATION, with its principal place of business at 150 Greenwich Street, New York, NY 10007 ("Covered Entity"), and THE NEW YORK CITY DEPARTMENT OF FINANCE ("DOF"), with its headquarters located at 1 Centre St, New York, NY 10007 ("Business Associate").

I. DEFINITIONS

Except as otherwise defined herein, any and all terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules (as defined below). As used in this Agreement, the following terms shall have the following meanings:

(a) **"Agreement"** shall mean the Health Insurance Portability and Accountability Act Business Associate Agreement Provisions constituting this Agreement.

(b) **"Breach"** shall have the same meaning as the term "breach" in 45 CFR §164.402.

(c) **"Business Associate"** shall have the same meaning as the term "business associate" in 45 CFR §160.103, and for this Agreement shall be the contractor or other person who is a party to the Agreement to which this is an Agreement and who may create, receive, maintain, transmit, or access Protected Health Information on behalf of Covered Entity pursuant to such Agreement. Business associates shall be referred to generically as "business associates."

(d) **"Covered Entity"** shall have the same meaning as the term "covered entity" in 45 CFR §160.103, and for this Attachment shall be the City agency that is a party to the Agreement to which this is an Attachment and constitutes a covered entity or has a health care component. Covered Entities shall be referred to generically as "covered entities."

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

(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) **"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.

(h) **"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.

(i) **"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).

(j) **"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 Business Associate or its Subcontractors or agents on behalf of Covered Entity.

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

(*l*) **"Secretary"** shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

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

(n) **"Subcontractor"** shall have the same meaning as the term "subcontractor" in 45 CFR §164.103, and for this Agreement shall be a subcontractor of Business Associate.

(o) **"Unsecured Protected Health Information"** or **"Unsecured PHI"** shall have the same meaning as the term "unsecured protected health information" in 45 CFR §164.402.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) **Permitted or Required Uses.** Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement and the MOU to which it is attached, or as Required By Law.

(b) **Appropriate Safeguards.** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement and the MOU to which it is attached, and with respect to Electronic Protected Health Information to comply with Subpart C of 45 CFR Part 164 (45 CFR §164.302 et seq.).

(c) **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effects of which Business Associate becomes aware that have resulted from any unauthorized acquisition, access, use or disclosure of Protected Health Information by Business Associate, its Subcontractors or agents.

(d) **Reporting Unauthorized Use or Disclosure.** Business Associate agrees to report to Covered Entity, in writing, any unauthorized acquisition, access, use or disclosure of Protected Health Information by Business Associate, its Subcontractors or agents in violation of this Agreement of which Business Associate becomes aware. Business Associate shall make such report to the designated representative of Covered Entity, in writing, within forty-eight (48) hours

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

(e) **Breach Notification Under HIPAA Rules.**

(1) 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, Business Associate shall, without unreasonable delay, and in no event later than sixty (60) days after discovery of any Breach of Unsecured PHI, notify Covered Entity in writing of any such Breach, unless a delay in such notification is required by 45 CFR §164.412. Business Associate shall provide Covered Entity with an explanation in writing of the basis for its determination that a Breach of Unsecured PHI has occurred 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.

(2) If Business Associate finds that an unauthorized acquisition, access, use or disclosure of PHI has occurred and has been reported to Covered Entity as required by Section II(d) or Section IV(c), but has been determined not to constitute a Breach of Unsecured PHI, Business Associate shall provide 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.

(3) Business Associate shall fully cooperate with any investigation conducted by Covered Entity or its designated agents of whether a Breach of Unsecured PHI has occurred. In the event of a disagreement between Business Associate and Covered Entity as to whether or not such a Breach has occurred, the determination made by Covered Entity shall control.

(4) Business Associate shall bear all costs related to its determination whether Business Associate has had a Breach of Unsecured PHI. In the event a Breach of Unsecured PHI has occurred, Business Associate shall reimburse Covered Entity for all costs incurred by Covered Entity related to: (i) providing the notice required by 45 CFR §§ 164.404 and 164.406, including if applicable, but not limited to, written notice, substitute notice, additional notice in urgent situations, and notification to media; and (ii) all measures in mitigation of the harmful effects of any acquisition, access, use, or disclosure of PHI that are commercially reasonable, including but not limited to, credit monitoring services for individuals affected by such Breach, and any other commercially reasonable preventive measure. The determination of whether a measure in mitigation of the harmful effects of any acquisition, access, use, or disclosure of PHI is commercially reasonable shall be in the sole discretion of the Covered Entity.

(f) **Subcontractors and Agents.** In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), as applicable, Business Associate agrees to ensure that all of its Subcontractors and agents that create, receive, maintain, transmit, or access Protected Health Information on behalf of Business Associate, agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information. Business Associate is not in

compliance with this Agreement if Business Associate knew of a pattern of activity or practice of a Subcontractor that constituted a material breach or violation of the Subcontractor's obligations under its subcontract, unless Business Associate took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the subcontract, if feasible.

(g) **Access by Individual.** Business Associate agrees to provide access, at the request of Covered Entity, and in the reasonable time and manner designated by the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual or Individual's designee in order to satisfy Covered Entity's obligations under 45 CFR §164.524, provided that Business Associate has Protected Health Information in a Designated Record Set.

(h) **Amendment to PHI.** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of 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 Business Associate has Protected Health Information in a Designated Record Set.

(i) **Request for an Accounting.** Business Associate agrees to document such disclosures of Protected Health Information, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528. 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(i) in order to provide an accounting of disclosures as necessary to satisfy Covered Entity's obligations under 45 CFR §164.528.

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

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

(*l*) **Access by Secretary to Determine Compliance.** Business Associate agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of Protected Health Information created, received, maintained, transmitted, or accessed by Business Associate on behalf of Covered Entity, available to the Covered Entity and to the Secretary, 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. Business Associate shall immediately notify Covered Entity upon receipt of any request by the Secretary for access and of all materials to be disclosed pursuant to such request.

III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

(a) **Use and Disclosure for Performance.** Except as otherwise provided in this Agreement, Business Associate may only use or disclose Protected Health Information as necessary to perform services, functions, activities, and/or duties for, or on behalf of, Covered Entity as specified in the MOU to which this is an Attachment, or as necessary to perform its duties under this Attachment, or as Required by Law, provided that such use or disclosure would not violate the HIPAA Rules if done by Covered Entity.

(b) **Disclosure to Third Parties.** Subject to Section II(f) and Section IV(b) of this Agreement, Business Associate may disclose Protected Health Information to third parties as necessary to perform services, functions, activities, and/or duties for, or on behalf of, Covered Entity as specified in the MOU to which this is an Attachment, or as necessary to perform its duties under this Attachment. 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 Associate herein.

(c) **Minimum Necessary Use and Disclosure.** In accordance with the HIPAA Rules, when using or disclosing Protected Health Information, or when requesting PHI from Covered Entity or another covered entity or business associate, 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.

(d) **Use for Management, Administration and Legal Responsibilities.** Business Associate may use Protected Health Information, if necessary, for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(e) **Disclosure for Management, Administration and Legal Responsibilities.** Business Associate may disclose Protected Health Information 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 (1) the disclosure is Required By Law, or (2) (A) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and (B) the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. 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, Business Associate shall notify Covered Entity of such pending disclosure and provide reasonable time for Covered Entity to oppose such disclosure, should Covered Entity deem such opposition necessary; provided, however, that if Covered Entity does not respond to Business Associate regarding such opposition prior to the date on which such disclosure must be timely made, Business Associate may, in its own discretion, disclose PHI as Required by Law or such lawful process.

(f) **Data Aggregation Services.** Business Associate may use or disclose Protected Health Information to provide data aggregation services relating to the health care operations of the Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B). Under no circumstances may

Business Associate disclose PHI to any other person or entity pursuant to this Section III(f) without the express authorization of Covered Entity.

(g) **De-identified PHI.** Business Associate agrees that it will obtain the prior approval of Covered Entity before de-identifying Protected Health Information in accordance with 45 CFR §164.514(a)–(c) and utilizing such de-identified PHI.

(h) **Use of PHI or De-identified PHI for Research Purposes.** Business Associate agrees that it will obtain the prior approval of Covered Entity for the use or disclosure of Protected Health Information or de-identified PHI for research purposes.

IV. SECURITY REQUIREMENTS

(a) **Safeguards to Protect Electronic PHI.** Business Associate agrees 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 Protected Health Information that Business Associate creates, receives, maintains, transmits, or accesses on behalf of Covered Entity.

(b) **Subcontractors and Agents.** In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), as applicable, Business Associate agrees to ensure that all of its Subcontractors and agents that create, receive, maintain, transmit, or access Electronic Protected Health Information on behalf of 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.

(c) **Reporting Security Incident.** Business Associate agrees to report to Covered Entity, in writing, any Security Incident involving Protected Health Information experienced by Business Associate, its Subcontractors or agents, of which Business Associate becomes aware. Business Associate shall make such report to the designated representative of Covered Entity, in writing, within forty-eight (48) hours of having been made aware of such Security Incident. Business Associate agrees to fully cooperate with any investigation conducted by Covered Entity or its designated agents of any such Security Incident.

V. COMPLIANCE WITH CERTAIN NEW YORK STATE LAWS

(a) **Confidentiality Under New York Law.** Business Associate agrees to comply with all applicable New York State laws and any regulations promulgated thereunder governing the confidentiality of information created, received, maintained, transmitted, or accessed by Business Associate, its Subcontractors or agents on behalf of Covered Entity, including but not limited to the following provisions, as applicable: 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; 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 New York General Business Law ("GBL") §899-aa(2) and (3) and in conformity with Section II(d) and Section IV(c) of this Agreement, Business Associate shall, within forty-eight (48) hours of discovery thereof, notify Covered Entity of any "breach of the security of the system," as defined in GBL §899-aa(1)(c), that involves Protected Health Information containing individuals' "private information," as defined in GBL §899-aa(1)(b), that was, or was reasonably believed to be, acquired from Business Associate, its Subcontractors or agents by a person without valid authorization. Business Associate shall bear all costs related to its "breach of the security of the system" under GBL §899-aa. In the event such breach has occurred, Business Associate shall reimburse Covered Entity for all costs incurred by Covered Entity related to providing the notice required by GBL §899-aa(5), including if applicable, but not limited to: written notice; electronic notice; telephone notification; substitute notice; email notice; posting of notice on web site; and notification to major statewide media.

VI. OBLIGATIONS OF COVERED ENTITY

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

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

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

(d) **Impermissible Request by Covered Entity.** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

VII. TERM AND TERMINATION

(a) **Term.** This Agreement shall be effective during the term of the MOU to which this is an Attachment, or until earlier termination of such MOU.

(b) **Termination for Violation of Material Term.** In the event that Covered Entity reasonably believes that Business Associate may have violated a material term of this Agreement, Covered Entity shall have the right to investigate such violation, and Business Associate shall fully cooperate with any such investigation. If Covered Entity determines that Business Associate has violated a material term of this Agreement, Covered Entity may immediately terminate the MOU to which this is an Attachment without penalty or recourse to Covered Entity. Alternatively, Covered Entity may provide written notice to Business Associate of the existence of a violation of

a material term of this Agreement, and afford Business Associate an opportunity to cure such violation to the satisfaction of Covered Entity within thirty (30) days of receiving notice of the violation or such other period of time as the parties may agree to. Failure to cure such violation within the applicable time period is grounds for immediate termination of the MOU to which this is an Attachment. If Covered Entity determines that neither cure of such violation nor termination is feasible, Covered Entity may report such violation to the Secretary and/or to any other governmental agency as may be required by applicable law, and Business Associate agrees that it shall not have or make any claim(s), whether at law or in equity, with respect to such report(s). Termination pursuant to this Section VII(b) shall be effectuated by a written notice to Business Associate that specifies the violation upon which the termination is based and the effective date of the termination.

(c) **Effect of Termination.**

(1) Except as provided in paragraph (2) of this Section VII(c), upon termination or expiration of the MOU to which this is an Attachment, Business Associate shall return or destroy, and ensure that its Subcontractors and agents return or destroy, all Protected Health Information received from Covered Entity, or created, maintained, received, or accessed by or on behalf of Business Associate or Covered Entity, that the Business Associate, its Subcontractors or agents still maintain in any form. Business Associate shall not retain, and shall ensure that its Subcontractors and agents not retain, copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon receipt by Covered Entity of such notification that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement, and shall ensure that its Subcontractors and agents in writing extend the same protections, to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate, its Subcontractors or agents, as applicable, maintain such Protected Health Information.

(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 MOU to which this is an Attachment and any other rights and remedies of the Covered Entity that are provided by law or by such MOU.

VIII. MISCELLANEOUS

(a) **Agency.** For purposes of this Agreement, it is the understanding and intention of the parties that Business Associate is acting as an independent contractor, and not an agent, of 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.** In order to ensure that this Agreement at all times remains consistent with applicable law and rules regarding use and disclosure of Protected Health Information (including but not limited to the HIPAA Rules), Business Associate agrees that this Agreement may be amended from time to time upon written notice from Covered Entity to Business Associate as to the revisions required to make this Agreement consistent with applicable law and rules.

(d) **Survival.** The respective rights and obligations of Business Associate and Covered Entity under the provisions of this Attachment shall survive the expiration or termination of the MOU to which this is an Attachment, unless this Agreement is specifically terminated in writing along with the MOU to which this is an Attachment.

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

(f) **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.