CNYCC BUSINESS ASSOCIATE AGREEMENT

INSTRUCTIONS PAGE

1. Page 1 – Please provide the following information: the date of signature, and the name of the Partner Organization;

2. Page 11 – Please provide the following information: the name of the Partner Organization, the signature of the authorized person to sign the BAA, and the authorized person's name and title. (Please note that Organization will have the option of completing signature requirement in either written or electronic form);

3. Please scan and send the executed Business Associate Agreement to dsripcarecollaborative@gmail.com by Friday November 13, 2015.

4. Please note - Attachment One (Page 12) to the BAA is a form required by the NYS Department of Health for any organization that receives Medicaid confidential data. It is an attestation about disposal of the data, **and should be filled out upon termination of the DSRIP project(s), not at present**.

Attachment B

RECIPROCAL BUSINESS ASSOCIATE AGREEMENT
BETWEEN CNYCC AND PARTNER ORGANIZATION

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into on the ___ day of _____, 2015 (the "Effective Date"), by and between Central New York Care Collaborative, Inc. ("CNYCC"), and [_____] ("Partner Organization"), each a "Party" and collectively the "Parties." This Agreement applies to the extent the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its implementing regulations, and the federal Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and its implementing regulations, apply to CNYCC and Partner Organization or if either Party receives from the other Party Medicaid Confidential Data (MCD). Nothing in this Agreement shall be construed to expand the applicability of HIPAA or the HITECH Act and the implementing regulations to the Parties hereto.

WHEREAS, CNYCC is the lead entity of a Performing Provider System (PPS) for purposes of the New York State Delivery System Reform Incentive Payment Program (DSRIP) and, along with its participating partner organizations ("Partner Organizations"), will develop and implement the CNYCC Project Plan to achieve DSRIP goals, which includes, among other things, creation of an integrated delivery system;

WHEREAS, Partner Organization has signed a Partner Organization Agreement with CNYCC to participate in the CNYCC network;

WHEREAS, the Parties possess individually identifiable health information which is subject to Applicable Privacy and Security Laws (defined below) and/or Medicaid Confidential Data (MCD) and may exchange individually identifiable health information between one another in furtherance of DSRIP-related activities, the flow of information being in both directions depending on the circumstances;

WHEREAS, in light of the dual flow and exchange of information, a Party may at times under this Agreement be acting as a "Covered Entity" because it is sharing information in its possession and the other Party receiving the information is its "Business Associate," or a Party may be acting as a Business Associate receiving the information from a Party that is the Covered Entity;

WHEREAS, depending on the flow of information, either Party may accordingly be referred to herein as "Covered Entity" (the Party sharing the information) and the other Party as "Business Associate" (the Party receiving the information);

WHEREAS, CNYCC has signed a Data Exchange Application and Agreement (DEAA) and Business Associate Agreement (the "CNYCC-DOH Agreements") with the New York State Department of Health ("DOH"), a "Covered Program" with respect to the use and sharing of MCD;

WHEREAS, when CNYCC is exchanging MCD as a Covered Entity with Partner Organization under this Agreement, the Parties understand that CNYCC is acting in the capacity of a Business Associate of DOH under the CNYCC-DOH Agreements, provided however, that for purposes of this Agreement, CNYCC's obligations are the same as those of a Covered Entity as set forth herein and Partner Organization is acting as CNYCC's subcontractor under the CNYCC-DOH Agreements and its obligations in receiving MCD from CNYCC are those of a Business Associate as set forth herein;

WHEREAS, when CNYCC has received protected health information as a Business Associate to a partner organization in the CNYCC Network, the Parties understand that CNYCC shall be deemed a Covered Entity under this Agreement when it shares that PHI with Partner Organization, and Partner Organization shall have the obligations of a Business Associate as set forth herein;

WHEREAS, when a Party is acting as a Covered Entity it seeks to require the Business Associate to appropriately safeguard individually identifiable health information;

WHEREAS, the Party acting as the Business Associate agrees to comply with all obligations imposed upon Business Associates under the Applicable Privacy and Security Laws; and

WHEREAS, the Parties desire to enter into this Agreement in order to comply with the Applicable Privacy and Security Laws and the CNYCC-DOH Agreements.

NOW, THEREFORE, in consideration of the mutual promises contained herein, the Parties hereto agree as follows:

1. Recitals. The terms of the recitals set forth above are hereby incorporated by this reference into this Agreement.

2. Defined Terms. Unless otherwise indicated below or elsewhere in this Agreement, all capitalized terms shall have the meanings as defined by HIPAA (see, 45 CFR 160.103, 164.103, 164.304, 164.402 and 164.501). For convenience, certain definitions are set forth below.

a. "Applicable Privacy and Security Laws" means HIPAA as defined below and any other applicable federal, state, and local laws and regulations that govern the creation, storage, receipt or transmission of individually identifiable medical records or information.

b. "Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule (as defined below) which compromises the security or privacy of the protected health information, subject to the exceptions provided in 45 CFR 164.402. For purposes of this definition, any acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy Rule shall be presumed to be a Breach unless it is demonstrated, through a risk assessment, that there is a low probability that the protected health information has been compromised.

c. "Covered Entity" means the Party that is sharing PHI with the other Party who is the Business Associate pursuant to this Agreement.

d. "HIPAA" means the final Privacy Rule issued pursuant to HIPAA (codified at 45 CFR Parts 160 and 164 as amended, modified, or superseded from time to time, ("Privacy Rule") and the final Security Rule issued pursuant to HIPAA (codified at 45 CFR Parts 160, 162 and 164 as amended, modified, or superseded from time to time, ("Security Rule"), as amended by the Health Insurance Technology for Economic Clinical Health Act ("HITECH"), and any amendments, regulations, rules and guidance issued pursuant to HITECH.

e. "Individual" means the person who is the subject of protected health information and shall include a person who qualifies as a personal representative under HIPAA (45 CFR § 164.502(g)).

f. "Medicaid Confidential Data" means any information or data derived from the Medicaid Analytics Performance Portal maintained by DOH about individuals who have applied for or receive Medicaid benefits, including Medicaid claims data, names and addresses, diagnoses, medical services, and other personally identifiable health information.

g. "Protected Health Information" or "PHI" means individually identifiable health information as defined by HIPAA (45 CFR 160.103), limited to the information received by Business Associate from Covered Entity or created or received by Business Associate on behalf of Covered Entity, which may include Medicaid Confidential Data (MCD) .

h. "Secretary" means the Secretary of the Department of Health and Human Services ("HHS") or his or her designee.

i. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

j. "Service Agreement" means the Partner Organization Agreement or other written, executed agreement between the Parties attached hereto, and any agreement subsequently executed between the Parties that entails the exchange of PHI or MCD for purposes of DSRIP.

k. "Unsecured PHI" means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5, as posted on the HHS web site.

3. Permitted Uses and Disclosures by Business Associate. Except as otherwise limited in this Agreement, Business Associate may use and/or disclose PHI received from, or created or received on behalf of Covered Entity to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in or required by the Service Agreement, provided that such use or disclosure would not violate: (i) Applicable Privacy or Security Laws; and (ii) requirements of the DEAA as set forth in Section 5 of this Agreement, including but not limited to CNYCC Policies and Procedures with respect to MCD. In the event of any conflict between this Agreement and the Service Agreement, this Agreement shall control.

4. Obligations and Activities of Business Associate.

a. Business Associate acknowledges and covenants that it shall comply with the provisions set forth in the Applicable Privacy and Security Laws and the requirements set forth in the DEAA with respect to MCD.

b. Use or Disclosure.

i. Subject to the further limitations set forth in Section 5 of this Agreement for any PHI that is MCD, Business Associate shall not use or further disclose PHI other than as permitted or required by this Agreement or as Required by Law.

ii. Business Associate may further use PHI for Business Associate's own proper management and administration or to carry out Business Associate's legal responsibilities**.**

iii. Business Associate may further disclose PHI for Business Associate's own proper management and administration, if disclosure is Required By Law or if Business Associate obtains reasonable assurances from the person to whom disclosure is to be made that it will be held confidentially and only further disclosed as Required By Law or for the purposes for which it was disclosed and the person to whom it was disclosed notifies Business Associate of any Breaches of confidentiality.

iv. Business Associate shall not use or further disclose PHI if Covered Entity would be prohibited from doing so if such use or disclosure was done by Covered Entity.

v. Business Associate shall use and disclose PHI in accordance with the minimum necessary standard of the Applicable Privacy and Security Law.

c. Safeguards. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI, including the implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity in accordance with the Security Rule.

d. Policies and Procedures. Business Associate shall implement written policies and procedures as appropriate to comply with and implement the standards and specifications required to comply with Applicable Privacy and Security Laws and this Agreement.

e. Reporting.

i. Business Associate shall use reasonable and diligent efforts to review and investigate any potential use or disclosure of PHI not provided for by this Agreement. Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for by this Agreement, of which it becomes aware within ten (10) calendar days of identifying the event. Business Associate shall determine and report any identified Breach to Covered Entity without unreasonable delay and no more than three (3) calendar days from identifying the Breach. Business Associate shall provide to Covered Entity such other available information as Covered Entity is required to include in a notification to individuals affected by the Breach and to the Secretary in accordance with 45 CFR § 164.404(c).

ii. Business Associate shall report verbally and in writing to Covered Entity any Security Incident of which it becomes aware within ten (10) days of identifying the

event. The notification shall identify the date of the Security Incident, the scope of the Security Incident, the Business Associate's response to the Security Incident and the identity of the person responsible for the Security Incident, if known, and such other available information as Covered Entity may request.

f. Agents and Subcontractors. Business Associate shall ensure that any agents or subcontractors: (i) to whom it provides PHI received from Covered Entity, or PHI created by or received from Business Associate on behalf of Covered Entity; or (ii) that create, receive, maintain, or transmit PHI on behalf of Business Associate shall agree in writing to comply with all provisions set forth in the Applicable Privacy and Security Laws, and shall agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI. No subcontractor or agent shall be permitted to use or disclose PHI received from Business Associate other than as permitted or required by this Agreement or as Required by Law. With respect to electronic PHI, where applicable, Business Associate shall notify and require any agents or subcontractors to implement appropriate security safeguards in accordance with the Security Rule. Business Associate shall obtain written assurances from agents and subcontractors that any of its agents or subcontractors that perform a function, service or activity that requires access to PHI shall agree to comply with the same requirements and safeguards as applicable to Business Associate.

g. Access. At the request of Covered Entity, Business Associate shall make available to Covered Entity or, as directed by Covered Entity, to an Individual, in a reasonable time and manner, access to PHI in a Designated Record Set (as such term is defined by HIPAA, 45 CFR § 164.501) in its possession related to the Individual to the extent required to comply with 45 CFR § 164.524. To the extent permitted by HIPAA, the obligations of Business Associate in this paragraph apply only to Designated Record Sets in Business Associate's possession or control.

h. Amendment. At the request of Covered Entity or the Individual, Business Associate shall make PHI or a record in a Designated Record Set available for amendment and to incorporate any amendments to said PHI or record in a reasonable time and manner in accordance with 45 CFR § 164.526. To the extent permitted by the Privacy Rule, the obligations of Business Associate in this paragraph apply only to Designated Record Sets in Business Associate's possession or control.

i. Accounting of Disclosures. Business Associate shall document disclosures as required under the Privacy Rule and information related to such disclosures to make available to Covered Entity or Individual an accounting of disclosures as required by the Privacy Rule (45 CFR § 164.528).

j. Governmental Access. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with 45 CFR Subpart C and to DOH for purposes of determining Business Associate's compliance with the restrictions related to access and use of MCD.

k. Risk Assessment. Business Associate shall immediately investigate any known or suspected Security Incident to determine whether the PHI was unsecured and compromises the security or privacy of the PHI. Business Associate shall provide Covered Entity, upon request, any document or information necessary for the Covered Entity to perform a similar risk assessment.

l. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect to impacted Individuals that is known to Business Associate or Covered Entity from a use or disclosure of unsecured PHI by Business Associate or its agents and subcontractors in violation of the requirements of this Agreement and Applicable Privacy and Security Rules. Business Associate shall provide Covered Entity, upon request, with any document or information necessary for Covered Entity to take similar reasonable and appropriate steps to mitigate the Breach. Business Associate shall document that the harmful effect was corrected to the extent possible and provide such documentation to Covered Entity for satisfactory assurance.

m. Breach Notification. Business Associate shall, upon determining a Breach has occurred, work with Covered Entity to notify the impacted Individuals, or as required under 42 USC § 17932, Media Outlets or the Secretary, of such a Breach without unreasonable delay and in no case later than sixty (60) calendar days after identifying the Breach with the information required under 45 CFR §§ 164.404; 164.406 and 164.408.

n. Audit. In the event of a government investigation or audit related to a Security Incident or Breach of PHI by Business Associate, Covered Entity shall manage any and all communications and responses with the investigators or auditors and control any and all issues related to a potential defense and settlement with the assistance and reasonable consideration of Business Associate.

o. Marketing: Except as otherwise provided in the Applicable Privacy and Security Laws, Business Associate shall not use or disclose PHI for the purposes of marketing and shall not directly or indirectly receive remuneration from a third party for making certain communications about a product or service that encourages the recipient to purchase or use the product or service unless an Individual has provided a valid, HIPAA-compliant authorization, including specification of whether the PHI can be further exchanged for remuneration by the receiving party.

p. Sale of PHI. Except as otherwise permitted in the Applicable Privacy and Security Laws, Business Associate shall not directly or indirectly receive remuneration in exchange for the disclosure of PHI, except pursuant to a valid HIPAA-compliant authorization stating that the disclosure will result in remuneration to the Business Associate.

q. Encryption. Business Associate may not transmit electronic PHI obtained from Covered Entity or created by Business Associate over any open network unless the data in such transmission is encrypted or secured from unauthorized access or modification in a manner that is consistent with 45 CFR § 164.312(e)(1) of the Security Rule, or guidance from the Secretary setting forth different or additional requirements or standards. Business Associate shall comply with standards for encryption for MCD, as set forth in CNYCC Policies and Procedures. For purposes of this section, the term “open network” includes the Internet, extranets (using Internet technology to link a business with information only accessible to collaborating Parties), leased lines, dialup lines, and private networks. For purposes of this section, the term "encryption" means the reversible coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key.

r. Applicable Laws. To the extent that Business Associate performs a function that applies to the Covered Entity, Business Associate will comply with the Applicable Privacy and Security Laws that apply to Covered Entity. To the extent that Business Associate engages in a covered

transaction, Business Associate shall comply with the electronic standard transaction rules in 45 CFR Part 162.

s. Required Written Authorizations. The Parties acknowledge that this Agreement is intended to supplement any and all other federal and state laws and regulations that impose obligations to maintain the confidentiality of PHI and MCD. Nothing in this Agreement will be construed to require or permit Business Associate to use or disclose PHI or MCD without a written authorization from an Individual or an Individual's authorized representative, where such authorization would be required under the applicable federal or state laws or regulations for such use or disclosure.

5. Medicaid Confidential Data: Obligations Arising from the DEAA.

a. CNYCC is covered under a Data Exchange Application and Agreement (DEAA) and addenda to the DEAA with DOH regarding storage and transmission of Medicaid Confidential Data (MCD). The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between DOH and any second party that will receive MCD must include contract language that will bind such parties to ensure that all contractors and subcontractors abide by the regulations and laws that govern the protection of individual MCD. This notification and the following language is required in this Agreement and for all future contracts that will govern the receipt and release of individual MCD, and is accordingly set forth in this Agreement:

Medicaid Confidential Data/Protected Health Information (MCD/PHI) includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information. Business Associate must comply with the following state and federal laws and regulations:

- *Section 367-b(4) of the NY Social Services Law*
- *New York State Social Services Law Section 369 (4)*
- *Article 27-F of the New York Public Health Law and 18 NYCRR 360-8.1*
- *Social Security Act, 42 USC 1396a (a)(7)*
- *Federal regulations at 42 CFR 431.302, 42 CFR Part 2*
- *The Health Insurance Portability and Accountability Act (HIPAA),at 45 CFR Parts 160 and 164*
- *Section 33.13 of the New York State Mental Hygiene Law.*

Please note that MCD released to 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), the following notice is provided to Business Associate:

"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."

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.

Business Associate agrees to ensure that 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 Associate agrees 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 Associate agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Business Associate enters into that involves MCD/PHI.

Neither Covered Entity, Business Associate nor any subcontractor may use or disclose MCD without the prior written approval of the New York State Department of Health.

b. Medicaid Confidential Data: Additional Obligations. CNYCC shall complete or assure completion of an Identity Assurance Assessment for each Business Associate that will store or process or have access to MCD provided by CNYCC. Business Associate agrees that prior to accessing MCD from CNYCC it shall: (i) cooperate fully in the Identity Assurance Assessment; (ii) implement the controls, including dual factor authentication and security standards and policies as required by New York State and Identity Assurance Assessment standards, for access to MCD from CNYCC; and (iii) sign a certification attesting to implementation of the required controls (Certification). Business Associate shall comply with CNYCC Policies and Procedures regarding MCD and the obligations of subcontractors set forth in the CNYCC-DOH Agreements.

6. Obligations and Activities of Covered Entity.

a. Covered Entity shall notify Business Associate of any limitation(s) or change in its notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify 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 impact Business Associate's use or disclosure of PHI.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

7. Term and Termination.

a. Term. This Agreement shall be effective as of the date first written above and shall continue until the Agreement is terminated in accordance with the provisions of this paragraph, or when the underlying Service Agreement between the Parties terminates.

b. Termination. Upon learning of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligation under this Agreement, Covered Entity may either:

i. Provide Business Associate with notice of and the opportunity to cure the breach or end the violation, as applicable, within a reasonable period of time but not later than twenty (20) days from notice and, if such steps are unsuccessful, terminate the Service Agreement and this Agreement, if feasible; or

ii. Terminate the Service Agreement and this Agreement immediately, if feasible.

c. Judicial or Administrative Proceedings. Either Party may terminate this Agreement, effective immediately, if: (i) the other Party is named as a defendant in a criminal proceeding for a violation of the Privacy Rule; or (ii) a finding or stipulation that the other Party has violated any applicable Privacy and Security Laws is made in any administrative or civil proceeding in which the Party has been joined.

d. Obligations upon Termination.

i. Business Associate shall, at the termination of this Agreement, if feasible, return or destroy all PHI received from, or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information. In the event that Business Associate determines that such return or destruction of PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible and extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

ii. If Business Associate has received MCD provided by CNYCC at any time during the term of this Agreement, Business Associate shall take all actions necessary, as determined by DOH, to comply with the Data Disposal Attestation Form Affidavit, attached as Attachment One, and shall complete and forward such form to CNYCC within thirty (30) days of termination of this Agreement.

iii. The provisions of this Section shall survive termination or expiration of this Agreement for any reason.

8. Indemnification. Each Party agrees to indemnify the other Party and its officers, directors, employees, agents, and subsidiaries for any and all claims, losses, liabilities, costs and expenses, including reasonable attorneys' fees and costs asserted or incurred in connection with the indemnifying Party's (a) failure to perform its obligations under this Agreement; (b) willful misconduct, negligent acts or omissions in carrying out the obligations under this Agreement or a Certification provided pursuant to Section 5(b) of this Agreement; or (c) the Party's violation of any Applicable Privacy and Security Laws. This indemnification obligation will survive the termination of this Agreement. Neither Party shall indemnify the other Party for the negligent acts or omissions of any other organization participating in the CNYCC PPS.

9. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement or the Privacy Rule will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate and its agents or subcontractors to safeguard the PHI.

10. Amendment.

a. Amendment to Comply with Law. The Parties acknowledge that state and federal laws relating to electronic data security and privacy and DOH guidance with respect to MCD are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such developments. The Parties agree to take such action as is necessary to implement the standards and requirements of the Applicable Privacy and Security Laws and DOH guidance with respect to MCD set forth in DEAA addenda or otherwise.

b. Amendment of Service Agreement. The Service Agreement may be modified or amended as provided in the Service Agreement by the Parties at any time without amendment of this Agreement.

11. No Third-Party Beneficiaries. This Agreement is intended for the sole benefit of Covered Entity and Business Associate and does not create any third party beneficiary rights, except as required under the Privacy Rule and as set forth in the DEAA.

12. Record Retention. Business Associate shall retain all records required to be created or retained under this Agreement for a period of no less than six (6) years following the date of termination of this Agreement or the Service Agreement, whichever is later.

13. Interpretation. This Agreement shall be interpreted as broadly as necessary to implement and comply with Applicable Privacy and Security Laws and the obligations imposed by the DEAA. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with Applicable Privacy and Security Laws and the DEAA.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement as of the date set forth above.

You have the option to sign this Agreement by hand or electronically. If you will sign this Agreement electronically, you must read the information below, follow the instructions, and check the box "I accept" to acknowledge the intent to use an electronic signature.

"I agree, and it is my intent, to sign this Agreement and affirmation by entering my name, preceded and followed by the forward slash (/) symbol (e.g., /John Doe/) and by electronically submitting this Agreement to CNYCC. I understand that my signing and submitting this Agreement in this fashion is the legal equivalent of having placed my handwritten signature on the submitted Agreement and this affirmation."

☐ accept

CNYCC	[INSERT NAME OF PARTNER ORGANIZATION]
By: _____	By: _____
Name: _____	Name: _____
Title: Executive Director	Title: _____

Attachment One
Business Associate Agreement

DATA DISPOSAL ATTESTATION FORM - AFFIDAVIT

1. My name is _____, and I reside at _____

2. I am employed at _____, which is located at _____

_____

3. Medicaid Confidential Data (MCD) and Protected Health Information (PHI) were obtained from CNYCC for the purposes or project (Project) set forth in the attached Business Associate Agreement (BAA).

This Project was completed on: _____.

4. I understand that use of the MCD and PHI for any purpose, other than the purpose stated in the underlying Service Agreement and/or the BAA is prohibited. As the Project has been completed, I understand that the MCD and PHI may no longer be used for any purpose whatsoever.

5. Please check one of the following responses regarding the return of MCD and PHI:

[ ] Previously returned on:_____ (Include copy of cover letter forwarding information)
[ ] Date to be returned: _____
[ ] Destroyed on: _____

6. I understand that there are civil and criminal penalties for violations of the following laws and regulations pertaining to the confidential nature of the Medicaid data:
   - Section 367b (4) of the NY Social Services Law
   - New York State Social Services Law Section 369 (4)
   - Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
   - Social Security Act, 42 USC 1396a (a) (7)
   - Federal regulations at 42 CFR 431.302; 42 CFR Part 2
   - The Health Insurance Portability and Accountability Act (HIPAA), at 45 CFR Parts 160 and 164.

7. I have retained none of the MCD/PHI disclosed to me under the above-referenced BAA and I understand that any MCD/PHI that I might recall from memory remains confidential.

State of _____ ss.:
County of _____

_____
SIGNATURE

Subscribed and sworn before me on this _____day of _____20_____.

_____
NOTARY PUBLIC