Better Health for Northeast New York, Inc.

POLICY FOR MEDICAID CONFIDENTIAL DATA

Approved by the BHNNY CEO on 5.29.2018

Purpose:

This Policy sets forth the obligation and procedures to maintain the confidentiality of Medicaid Confidential Data as required in the Data Use Agreement ("DUA") entered into between Better Health for Northeast New York, Inc. ("BHNNY") and the New York State Department of Health. The Policy also covers security incident and breach reporting obligations for Medicaid Confidential Data.

Definitions:

Terms that are capitalized in this Policy shall have the meanings as set forth below.

"Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule (codified at 45 CFR Parts 160 and 164) 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.

"Contractor" means any organization that provides services to BHNNY, or a subcontractor of such organization, that has access to MCD as a result of providing the services.

"**Custodian**" means the person appointed by BHNNY or by a Contractor of BHNNY to control and track access to MCD, as set forth in this Policy.

"Data Repository" means the repository of data, including MCD, maintained by Health Catalyst at 522 Delong Street, Salt Lake City, Utah (or any location to which Health Catalyst may subsequently transfer the Data Repository) on behalf of BHNNY for data analytics to implement DSRIP projects and goals.

"DOH" means the New York State Department of Health.

"**Downstream Partner Organization**" means a Partner Organization in the BHNNY Performing Provider System ("PPS") that receives MCD electronically or in paper form from BHNNY to provide treatment or care coordination services for such Partner Organization's patients who are also attributed to BHNNY.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated pursuant thereto, each as amended from time to time.

"Medicaid Confidential Data" or "**MCD**" means data about Medicaid beneficiaries derived from Medicaid data maintained and provided to BHNNY by New York State, including data from the MAPP database, Salient Interactive Miner, MAPP 2.0, the Medicaid Claims File, and PSYCKES, that is Protected Health Information within the meaning of HIPAA.

"PHI" means Protected Health Information as such term is defined in HIPAA.

"Security Incident" for purposes of this Policy means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices as applicable to MCD.

"Workforce Members" means employees and contractors of an organization.

POLICY

BHNNY is a party to the DUA and Business Associate Agreement (BAA) with DOH for the purpose of permitting BHNNY to receive and access MCD to carry out its functions as the lead entity of the BHNNY PPS. The DUA permits BHNNY to provide MCD to Contractors of BHNNY and to Downstream Partner Organizations, in accordance with the terms and conditions in the DUA. BHNNY and its Business Associates, including Contractors and Downstream Partner Organizations, shall strictly comply with the requirements of this Policy.

This Policy adds to, but does not replace, the privacy and security policies of BHNNY, Contractors, and Downstream Partner Organizations and the obligation to comply with HIPAA and all other applicable federal and state privacy laws and regulations. The Policy incorporates certain requirements of the DUA. BHNNY, Contractors, and Downstream Partner Organizations are also bound by the terms of the Business Associate Agreement ("BAA") between BHNNY and each respective organization, except where the BAA conflicts with specific requirements of this Policy regarding Security Incident and Breach Reporting for MCD, as set forth below.

I. GENERAL REQUIREMENTS

1. BHNNY shall only provide MCD to individuals or organizations, consistent with the minimum necessary rule of HIPAA and the statement of purpose for data use ("Statement of Purpose") in the DUA, attached as Appendix A. Contractors and Downstream Partner Organizations that receive MCD may only disclose it to individuals within their own organizations in accordance with the HIPAA minimum necessary rule and the Statement of Purpose.

2. The BHNNY Custodian shall seek the approval of DOH to share MCD with each new organization that will have access by submitting a DUA Addendum to DOH. Contractors and Partner Organizations shall not share MCD provided by BHNNY,

including MCD that has been commingled with other data, with any other organization without the approval of the BHNNY Custodian.

3. If MCD is commingled in a database with other data, that database shall also be treated as MCD. Access to the database shall be managed in accordance with this Policy, including the requirements for destruction of MCD in the database.

4. MCD shall not be accessed by BHNNY Workforce Members, Contractors or Downstream Partner Organizations who are located outside the United States or its territories.

5. BHNNY Contractors and Downstream Partner Organizations shall have established appropriate administrative, technical, and physical safeguards to protect the confidentiality of PHI and MCD and to prevent unauthorized use of or access to such data. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by HIPAA.

6. In accordance with the DUA, MCD in any form, e.g., paper copies, electronic medium, shall be returned to DOH or destroyed, as required by DOH, upon the completion of the purpose for using the MCD.

7. Copies of MCD in paper form shall be kept locked in a secure location when not in use. Paper copies shall be destroyed by shredding in a process that meets the requirements of HIPAA and assures that the data cannot be reconstructed. MCD stored in any electronic medium shall also be deleted in accordance with the requirements of HIPAA.

II. CUSTODIAN RESPONSIBILITIES

A. Appointment and Duties of BHNNY Custodian and Alternate Custodian

1. BHNNY will designate an individual to carry out the duties of Custodian as stated in this Policy and an Alternative Custodian to carry out the Custodian's duties in the event that the Custodian is not available. BHNNY shall report any change in the Custodian or Alternate Custodian to the Security and Privacy Bureau at DOH within fifteen (15) days of the change by submitting a notarized DUA Addendum.

2. The Custodian shall be responsible for creating and maintaining an accurate list of all Workforce Members at BHNNY and Contractors who have access to MCD from the Data Repository established for BHNNY, or have access to MCD in any other form, including paper copies. The Custodian shall coordinate with BHNNY senior staff as well the Custodian at each Contractor to maintain the required list of individuals with access to MCD.

3. The Custodian shall report all changes in BHNNY and Contractor Workforce Members who have or will have access to MCD in a quarterly report

("Quarterly Names Update") to the Security and Privacy Bureau at DOH. Such list shall contain the first and last names and employment start and end dates of all affected Workforce Members of BHNNY and Contractors with access to MCD. The Quarterly Names Update will be accompanied by a notarized DUA Addendum. In addition to the Quarterly Names Update, the Custodian will notify the Security and Privacy Bureau of all changes in the BHNNY Workforce Members with access to MCD within twenty-four (24) hours. The Custodian will provide the list of BHNNY and Contractor Workforce Members with access to MCD to DOH upon written request or audit by DOH at any time.

4. The Custodian shall be responsible for compliance with the requirements of the DUA in coordination with the BHNNY Chief Information Security Officer and Chief Compliance Officer. The BHNNY Custodian shall oversee compliance with this Policy by Contractors and Downstream Partner Organizations, and shall oversee training for BHNNY Workforce Members who will have access to MCD about the safeguards that apply to MCD.

5. The Custodian shall be responsible for approving access for each new Contractor or Downstream Partner Organization that will be given access to or will receive MCD or reports containing MCD, and for submitting a DUA addendum to DOH seeking approval of such access, as necessary. The Custodian will provide to DOH upon request all policies and procedures related to BHNNY access management to MCD, including provisioning, modifying, and terminating users who access any system that stores, processes, analyzes or transmits MCD on behalf of BHNNY.

B. Custodian for Third Party Contractors

1. Any Contractor that receives MCD from BHNNY shall designate an individual to serve as custodian ("Contractor Custodian") who will be responsible for controlling the dissemination of MCD within the Contractor organization and identifying all individuals who have access to MCD. The Contractor Custodian shall sign the certification attached as Appendix B to this Policy, and shall provide a copy of the signed certification to the BHNNY Custodian, upon request.

2. The Contractor Custodian shall provide to the BHNNY Custodian a list of all individuals who have access to MCD, and shall report the names of any individuals with access to MCD who join or leave the Contractor workforce within seven (7) days of the change. Such information shall be included in the Quarterly Names Update.

3. The Contractor Custodian shall oversee and be responsible for access to MCD by Contractor's Workforce Members, and shall review the need for access by each individual in accordance with the HIPAA minimum necessary rule and the Statement of Purpose prior to granting access to the

Workforce Member. Only the Contractor Custodian, in consultation with the BHNNY Custodian as necessary, shall be authorized to grant access to MCD by Workforce Members. The Contractor Custodian shall also be responsible for providing training about the physical, technical, and administrative safeguards in effect at Contractor to protect the confidentiality of MCD, for overseeing implementation of the safeguards, and for assuring the destruction or return of all MCD as required by the DUA.

4. The Contractor Custodian shall be responsible for providing to each Workforce Member who will be granted access to MCD a copy of this Policy and the organization's privacy and security policies that apply to access, use, transmission and disclosure of MCD. The Contractor Custodian shall also assure that Workforce Members who will access MCD receive training about the safeguards that apply to MCD. No person may be granted access to MCD by a Contractor until such person has signed the attached certification (Appendix C) acknowledging that he/she has reviewed the privacy and security policies that apply to MCD and agrees to abide by such policies and by this Policy. It shall be the responsibility of the Contractor Custodian to obtain executed certifications, as applicable, and to retain copies of such certifications. Contractor Custodian shall provide copies of executed certifications to BHNNY, upon request.

C. Reporting and Oversight of Access by Downstream Partner Organizations to MCD

1. Each Downstream Partner Organization that receives reports that contain MCD from BHNNY shall designate a privacy/security or compliance officer to oversee the dissemination of MCD within its organization ("Designated MCD Representative") in accordance with this Policy and the BAA with BHNNY, as updated by the addendum to the BAA signed by BHNNY and the Downstream Partner Organization.

2. The Designated MCD Representative shall establish and maintain a list of the Workforce Members granted access to MCD, in any form, e.g., paper, electronic, provided by BHNNY and shall update the list periodically as Workforce Members with access to MCD change. This list of Workforce Members with access to MCD shall be maintained by the Designated MCD Representative and shall be relied upon to assure destruction or return of all MCD in accordance with the DUA. The list shall be provided to BHNNY, upon request.

3. The Designated MCD Representative shall be responsible for providing information and training to Workforce Members granted access to MCD about the physical, technical and administrative safeguards at the Partner Organization to protect the confidentiality of MCD, and for overseeing implementation of the safeguards.

III. SECURITY INCIDENT AND BREACH REPORTING FOR MCD

The provisions in the BAA entered into between BHNNY and each of its respective Business Associates for security incident and breach reporting remain in effect as do all requirements of HIPAA, which shall apply for security incidents and Breaches that involve PHI that is not MCD.

This Policy incorporates the requirements of the DUA in relation to Security Incident and Breach reporting, investigation, and remediation for MCD. For Security Incidents or Breaches that entail MCD, this Policy applies and overrides any conflicting provisions of the BAA between BHNNY and its Contractors or Downstream Partner Organizations.

A. BHNNY'S OBLIGATIONS

1. BHNNY shall report to DOH any Breach involving personally identifiable information (PII) or PHI that is MCD by e-mail notification at doh.sm.Medicaid.Data.Exchange@health.ny.gov within one (1) hour of: (a) the time that BHNNY determines that a Breach has occurred within its information systems or as a result of the actions of a BHNNY Workforce Member; or (b) a Contractor or Downstream Partner Organization reports to BHNNY that a Breach of MCD has occurred. If DOH determines that the risk of harm requires notification of affected persons of the Breach and/or other remedies, BHNNY shall carry out such notifications and/or other remedies, or require its Contractors or Downstream Partner Organizations to do so, as appropriate.

2. If BHNNY determines that a Security Incident has occurred in one of its information systems, BHNNY shall inform DOH promptly once it has determined the nature of the Security Incident and if the Security Incident actually entailed an unauthorized disclosure of or access to MCD. DOH may require BHNNY to complete a risk analysis, risk assessment, or an organizational attestation affirming that BHNNY has identified and remediated the root cause of the cyberattack or other cause of the Security Incident and that its information systems and networks have been remediated and have returned to normal operation.

3. If DOH determines or believes that BHNNY has used, reused, or disclosed MCD in a way other than as explicitly authorized by the DUA, BHNNY shall do the following, if requested by DOH:

    a. Promptly investigate and report to DOH BHNNY's determinations regarding any alleged or actual unauthorized use, reuse or disclosure;

    b. Promptly resolve any problems identified by the investigation;

    c. Submit a formal response to an allegation of unauthorized use, reuse or disclosure;

d. Submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and

e. Destroy all data files received from DOH and submit a data destruction affidavit.

4. BHNNY shall conduct a forensic investigation for any significant Security Incident that arises in its information systems. Prior to the start of such investigation, BHNNY shall determine how it will collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. BHNNY shall make all such decisions in accordance with its policies and advice from legal counsel. In such situations, BHNNY shall follow a clearly defined chain of custody to avoid allegations of mishandling or tampering with evidence, and shall 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.

5. BHNNY shall make and retain a forensic copy of the evidence and verify the integrity of both the original and the copied evidence. BHNNY shall 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 shall be preserved. All forensic examination, such as that described above, must account for the disposition and impact on all MCD as well as all systems that store, process, analyze, or transmit MCD in any report that may be required by DOH.

B. OBLIGATIONS OF CONTRACTORS AND DOWNSTREAM PARTNER ORGANIZATIONS

1. Contractors and Downstream Partner Organizations shall report to the BHNNY Chief Compliance Officer, the BHNNY Compliance Officer, or the BHNNY Custodian within one (1) hour of determining that a Breach or disclosure of MCD to an unauthorized person(s) has occurred. Contractors and Downstream Partner Organizations shall immediately undertake an investigation and review of the Breach upon making a determination that a Breach has occurred, and cooperate fully with BHNNY in the investigation and review process, as requested by BHNNY. If DOH or BHNNY determines that the risk of harm arising from the Breach of MCD requires notification of affected individuals of the Breach and/or other remedies, or if such notice is required by HIPAA, then at BHNNY's election either: (i) BHNNY shall carry out the notifications and/or other remedies with the cooperation of the Contractor or Downstream Partner Organization; or (ii) the Contractor or Downstream Partner Organization shall carry out the notifications and/or other remedies at the direction of BHNNY.

2. If a Contractor or Downstream Partner Organization determines that a Security Incident has occurred involving MCD in one of its information systems, Contractor or Downstream Partner Organization shall inform BHNNY within ten (10) business days of discovering the Security Incident. The Contractor or Downstream Partner Organization shall contact BHNNY as above, if a determination is made that the Security Incident entailed a Breach or disclosure of MCD to an unauthorized person.

3. BHNNY shall inform DOH of any reported Security Incident involving MCD reported by a Contractor or Downstream Partner Organization. At the request of DOH or otherwise, BHNNY may require a Contractor or Downstream Partner Organization to complete a risk analysis and a risk assessment. If required by DOH, the Contractor or Downstream Partner Organization shall prepare an organizational attestation affirming that the organization has identified and remediated the root cause of the cyberattack or other cause of the Security Incident and that its information systems and networks have been remediated and have returned to normal operation. BHNNY may suspend or terminate access to MCD through the Data Repository or otherwise, until the organizational attestation has been accepted by DOH and BHNNY has determined that remediation has been completed.

4. If DOH or BHNNY determines that a Contractor or Downstream Partner Organization has used, reused, or disclosed MCD in a way other than as explicitly authorized by the DUA or in violation of HIPAA or other applicable privacy and security laws and regulations, Contractor or Downstream Partner Organization shall do the following, if requested by DOH or by BHNNY:

    a. Promptly investigate and report to BHNNY its determinations regarding any alleged or actual unauthorized use, reuse or disclosure;

    b. Promptly resolve any problems identified by the investigation;

    c. Prepare a formal response to an allegation of unauthorized use, reuse or disclosure for submission to DOH, if requested by DOH;

    d. Submit a corrective action plan to BHNNY for submission to DOH with steps designed to prevent any future unauthorized uses, reuses, or disclosures; and

    e. Destroy all data files received from DOH and submit a data destruction affidavit to DOH.

5. Contractor or Downstream Partner Organization shall conduct a forensic investigation for any significant Security Incident. Prior to the start of such investigation, Contractor or Downstream Partner Organization shall

determine how it will collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings and shall make all such forensic decisions in accordance with its policies and advice from legal counsel. In such situations, Contractor or Downstream Partner Organization shall follow a clearly defined chain of custody to avoid allegations of mishandling or tampering with evidence, and shall 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.

6. Contractor or Downstream Partner Organization shall: (i) make and retain a forensic copy of the evidence and verify the integrity of both the original and the copied evidence; (ii) assure that the original evidence is stored securely; and (iii) perform all forensic examination and analysis using only the copied evidence. If it is unclear whether or not evidence preservation is required, the evidence shall be preserved. The forensic examination must account for the disposition and impact on all MCD as well as all systems that store, process, analyze, or transmit MCD. Contractor or Downstream Partner Organization shall prepare and submit a report to DOH about the Security Incident, if required to do so.

APPENDIX A

STATEMENT OF PURPOSE FOR DATA USE*

In consideration for accepting the data file(s) that include Medicaid Confidential Data ("MCD"), BHNNY represents that such data file(s) will be used solely for the purpose(s) listed below. BHNNY 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 BHNNY and DOH. BHNNY affirms that the data requested by BHNNY is the minimum necessary to achieve the purposes stated in this section. BHNNY agrees that, within BHNNY's organization and the organizations of its business associates, access to the data covered by the DUA shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated below.

Access to MCD by PPS Project Management Office

The purpose of the DUA is to permit BHNNY, as PPS lead, access to, and ability to share, a variety of demographic and clinical variables needed to help identify greatest areas of need in terms of Medicaid redesign activities associated with implementation of the Delivery System Reform Incentive Payment program, as promulgated by the DOH, subject to the 1115 Waiver requirements imposed by CMS. BHNNY staff will continue to utilize MAPP and Salient Interactive Miner along with obtaining access to the Medicaid Claims Files via our analytics application, to support DSRIP goals and the above mentioned initiatives. Receipt and use of this data is critical to assist Medicaid beneficiaries located throughout the five-county service area.

Access to MCD will be used to generate reports on prevalence rates on any of BHNNY's performance measures and quality indicators based on all the provider partners within the PPS network and on beneficiaries attributed to BHNNY PPS. The MCD data will allow the BHNNY Project Management Office staff to drill-in to view a list of beneficiaries served by a specific provider selected, who meet criteria for a selected quality flag, and to work with those providers to address specific areas of quality concern.

Substantial benefits will ensue to the State in terms of improved care coordination and reduced expense due to avoidable utilization of hospitals and emergency rooms. Beneficiaries will benefit from having improved access to care, treatment plan development, integration and co-location of services, and improved quality. The taxpayer will benefit by a reduction in public spending because of savings accrued from reduced service utilization. Rigorous controls are in place to ensure that data will be securely managed, logs of who accessed data will be maintained, no data will be shared with unapproved or unauthorized users. BHNNY will strictly adhere to all relevant internal policies and procedures, applicable State and federal regulations and laws.

* This statement is an excerpt from the Data Use Agreement between BHNNY and the New York State Department of Health ("DOH"). It binds BHNNY and all the organizations that receive MCD from BHNNY.

Access to PSYCKES

The PPS Project Management Office staff will obtain access to the Office of Mental Health PSYCKES application to support DSRIP goals. The PSYCKES PPS access will be used to review reports on prevalence rates on any of the quality indicators in PSYCKES based on all of the provider partners within the PPS network and based on clients attributed to their PPS. The PSYCKES application will allow a PPS user to drill-in to view a list of clients attributed to their PPS, served by a specific provider selected, who meet criteria for a selected quality flag. This access will allow a PPS user to view the same information that their provider partners can view in PSYCKES and therefore have actionable data on clients to work with to address specific areas of quality concern. The PPS network access user will also have the ability to obtain client consent for accessing PSYCKES data so that PPS network users can have access to all available data in a client's clinical summary (including data with special protection such as substance use information). Clients who have opted out of DSRIP will not be considered part of the attributed lives cohort when PSYCKES releases client-level data to the PSYCKES PPS user.

APPENDIX B

Custodian Certification Form for Access to Medicaid Confidential Data

By signing below, I certify as true and correct all of the following:

1) I understand that I will be granted access to Medicaid Confidential Data ("MCD") either in electronic and/or paper form.

2) I understand that MCD may only be used for specified purposes, and I agree to use MCD only for the limited purposes of which I have been granted access and in accordance with the minimum necessary rule of HIPAA.

3) I understand that it is my responsibility to protect the privacy and security of MCD. I have received training about the safeguards to protect the confidentiality of MCD. I have read and agree to comply with the Better Health for Northeast New York Medicaid Confidential Data (BHNNY MCD) Policy.

4) I understand and agree that I am not permitted to make additional copies, further share MCD with non-authorized users of MCD or non-authorized entities, either in paper or electronic means, or combine MCD with another database or information sharing and retrieval system, except with the express approval of the person designated to make such decisions in my organization. I agree to abide by this limitation and with policies that apply to the storage and disposal of MCD.

5) I have been appointed as Custodian at my organization and agree to fulfil the responsibilities of Custodian as stated in the BHNNY MCD Policy.

_____ _____

Print Name of Custodian Date

_____

Signature of Custodian

_____

Title

_____

Name of Organization

APPENDIX C

Individual Certification Form for Access to Medicaid Confidential Data

By signing below, I certify as true and correct all of the following:

1) I understand that I will be granted access to Medicaid Confidential Data ("MCD") either in electronic and/or paper form.

2) I understand that MCD may only be used for specified purposes, and I agree to use MCD only for the limited purposes of which I have been granted access and in accordance with the minimum necessary rule of HIPAA.

3) I understand that it is my responsibility to protect the privacy and security of MCD. I have received training about the safeguards to protect the confidentiality of MCD. I have read and agree to comply with the BHNNY MCD Policy.

4) I understand and agree that I am not permitted to make additional copies, further share MCD with non-authorized users of MCD or non-authorized entities, either in paper or electronic means, or combine MCD with another database or information sharing and retrieval system, except with the express approval of the person designated to make such decisions in my organization. I agree to abide by this limitation and with policies that apply to the storage and disposal of MCD.

_____ _____

Print Name of Individual Date

_____

Signature of Individual

_____

Title

_____

Name of Organization