DATA USE AGREEMENT

BETWEEN

THE DISTRICT OF COLUMBIA DEPARTMENT OF HEALTH CARE FINANCE

AND

_____

For the purpose of this Data Use Agreement ("DUA"), herein referred to as "The Agreement", **the Department of Health Care Finance (DHCF)** will be referred to as "DHCF" and _____, as a recipient of Protected Health Information ("PHI") or electronic PHI from DHCF, herein referred to as "*RECIPIENT*".

Instructions: Please check if this DUA is for a specific type of data set. See definitions in Appendix B.

☐ De-identified Data Set
☐ Limited Data Set
☐ Masked or Pseudo-anonymized Data Set

(Insert a brief description of the RECIPIENT and the data sharing Scope of Work activities proposed under this DUA.)

_____
_____
_____
_____
_____
_____
_____
_____
_____

Terms used, but not otherwise defined, in this DUA shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act ("HIPAA") Regulations.

1. Definitions

a. *Business Associate* means a person or entity, who, on behalf of the District or of an Organized Health Care Arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the Workforce of the District government or Organized Health Care Arrangement, creates, receives, maintains, or transmits PHI for a function or activity for the District, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R § 3.20, billing, benefit management, practice management, and repricing; or provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation (as defined in 45 C.F.R § 164.501), management, administrative, accreditation, or financial services to or for the District, or to or for an Organized Health

Care Arrangement in which the District participates, where the provision of the service involves the disclosure of PHI from the District or arrangement, or from another Business Associate of the District or arrangement, to the person. A Covered Entity may be a Business Associate of another Covered Entity.

A Business Associate includes, (i) a Health Information Organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI; (ii) a person that offers a personal health record to one or more individuals on behalf of the District; (iii) a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

A *Business Associate* does not include: (i) a health care provider, with respect to disclosures by a Covered Entity to the health care provider concerning the treatment of the individual; (ii) a plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or health maintenance organization, HMO, with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 C.F.R § 164.504(f) apply and are met; (iii) a government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law; (iv) a Covered Entity participating in an Organized Health Care Arrangement that performs a function, activity or service included in the definition of a Business Associate above for or on behalf of such Organized Health Care Arrangement.

b. *Covered Entity* means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by 45 C.F.R. §§ 160 and 164. With respect to this DUA, *Covered Entity* shall also include the designated Health Care Components of the District government's Hybrid Entity or a District agency following HIPAA's implementing regulations and best practices.

c. *Covered Functions* means those functions of a Covered Entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

d. *Data Aggregation* means, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.

e. *Designated Record Set* means a group of records maintained by or for a Covered Entity that are:

   i. The medical records and billing records about individuals maintained by or for a covered health care provider;

   ii. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

   iii. Records used, in whole or in part, by or for the Covered Entity to make decisions about individuals.

f. *Health Care* means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

i. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

ii. Sale or dispensing of a drug, device, equipment, or other item in accordance with the prescription.

g. *Health Care Components* means a component or a combination of components of a Hybrid Entity designated by a Hybrid Entity in accordance with 45 CFR § 164.105(a)(2)(iii)(D). *Health Care Components* must include non-Covered Functions that provide services to the Covered Functions for the purpose of facilitating the sharing of PHI with such functions of the Hybrid Entity without Data use agreements or individual authorizations.

h. *Health Care Operations* shall include (1) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R § 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) except as prohibited under 45 C.F.R. § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable; (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) business management and general administrative activities of the entity, including, but not limited to: (i) management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer; (iii) resolution of internal grievances; (iv) the sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and (v) consistent with the applicable requirements of 45 C.F.R. § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.

i. *Hybrid Entity* means a single legal entity that is a Covered Entity and whose business activities include both covered and non-Covered Functions, and that designates Health Care Components, in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C). A *Hybrid Entity* is required to designate Health Care Components, any other components of the entity that

provide services to the Covered Functions for the purpose of facilitating the sharing of PHI with such functions of the Hybrid Entity without Data use agreements or individual authorizations. The District is a Hybrid Covered Entity. Hybrid Entities are required to designate and include functions, services and activities within its own organization, which would meet the definition of Business Associate and irrespective of whether performed by employees of the Hybrid Entity, as part of its Health Care Components for compliance with the Security Rule and privacy requirements under this DUA.

j. *Individual* shall mean the person who is the subject of PHI in accordance with 45 C.F.R. § 160.103. The term *individual* shall also include the individual's personal representative in accordance with 45 C.F.R. § 164.502(g).

k. *Individually Identifiable Health Information* shall mean information that is a subset of health information, including demographic information collected from an individual, and;

   i. Is created or received by a health care provider, health plan, employer, or health care clearinghouse;

   ii. Relates to the past, present, or future physical or mental health or condition of an individual; or the past, present, or future payment for the provision of health care to an individual; and

   iii. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

l. *National Provider Identifier (NPI)* shall mean the Standard Unique Health Identifier for Healthcare Providers as defined at 45 C.F.R. § 162.406.

m. *Organized Health Care Arrangement* shall mean (1) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) an organized system of health care in which more than one Covered Entity participates and in which the participating Covered Entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (a) utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf; (b) quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or (c) payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk in accordance with 45 C.F.R. § 160.103.

n. *Personal Representative:* shall mean a person authorized, under District or other applicable law, to act on behalf of the subject of PHI in accordance with 45 C.F.R. § 164.502(g).

o. *Privacy and Security Official:* shall mean the person or persons designated by the District, a Hybrid Entity, who is/are responsible for developing, maintaining, implementing and enforcing the District-wide Privacy Policies and Procedures, and for overseeing full compliance with HIPAA Regulations, and other applicable federal and state privacy laws.

p. *Privacy Officer* shall mean the person designated by the District's Privacy and Security Official or one of the District's covered components within its Hybrid Entity, who is responsible for overseeing compliance with a Covered Agency's Privacy Policies and Procedures, the HIPAA Regulations and other applicable federal and state privacy laws. Also referred to as the agency Privacy Officer, the individual shall follow the guidance of the District's Privacy and Security Official, and shall be responsive to and report to the District's Privacy and Security Official on matters pertaining to HIPAA compliance.

q. *Privacy Rule* shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. parts 160 and 164, subparts A and E.

r. *Protected Health Information ("PHI")* means individually identifiable health information, including electronic information ("ePHI"), that is created or received by the Business Associate from or on behalf of the Covered Entity, or agency following HIPAA best practices, which is:

i. Transmitted by, created or maintained in electronic media; or

ii. Transmitted or maintained in any other form or medium;

iii. PHI or ePHI does not include individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) In records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (iii) In employment records held by a Covered Entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.

s. *Record* shall mean any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.

t. *Required By Law* means a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits pursuant to 45 C.F.R. § 164.103.

u. *Secretary* means the person serving as Secretary of the United States Department of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.

v. *Security Officer* means the person designated by the Security Official or one of the District of Columbia's designated Health Care Components, who is responsible for overseeing compliance with the Covered Agency's Privacy Policies and Procedures, the Security Rules, and other applicable federal and state privacy law(s). The Covered Agency's security officer shall follow the guidance of the District's Security Official, as well as the Associate Security Official within the Office of the Chief Technology Officer, and shall be responsive to the same on matters pertaining to HIPAA compliance.

w. *Security Rule* shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. parts 160, 162 and 164, subpart C.

x. Unsecured PHI shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the U.S. Department of Health and Human Services Secretary in the guidance issued under § 13402(h)(2) of the Health Information Technology Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA)(Pub.L 111-5, 123 Stat 115), approved February 17, 2009.

y. *Workforce* shall mean employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or RECIPIENT, is under the direct control of such Covered Entity, whether or not they are paid by DHCF or RECIPIENT.

2. Obligations and Activities of RECIPIENT

RECIPIENT agrees to comply with applicable federal and District confidentiality and security laws, including, but not limited to the Privacy Rule and Security Rule and the following:

a. RECIPIENT agrees not to use or disclose PHI or ePHI (other than as permitted or required by this DUA or as Required By Law.

b. RECIPIENT agrees to use appropriate safeguards and comply with administrative, physical, and technical safeguards requirements described at 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 as required by § 13401 of the Health Information Technology Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA")(Pub.L 111-5, 123 Stat 115) approved February 17, 2009, to maintain the security of the PHI and to prevent use or disclosure of such PHI other than as provided for by this DUA. RECIPIENT acknowledges that, pursuant to § 13401 of the HITECH, RECIPIENT must comply with the Security Rule and privacy provisions detailed in this DUA.

The additional requirements of § 13401 of HITECH that relate to security and apply to a Covered Entity shall also apply to RECIPIENT and shall be incorporated into this an agreement between RECIPIENT and DHCF. RECIPIENT shall be directly liable for any violations of this DUA or HIPAA Regulations. A summary of HIPAA Security Standards for the Protection of ePHI, found at Appendix A to Subpart C or 45 C.F.R. Part 164 is as follows:

Administrative Safeguards

R= Required and A = Addressable

Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A)

		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards

Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Technical Safeguards (see § 164.312)

Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

c. RECIPIENT agrees to name a Privacy and/or Security Officer who is accountable for developing, maintaining, implementing, overseeing the compliance of and enforcing compliance with this DUA, the Security Rule and other applicable federal and state privacy law within RECIPIENT's business. RECIPIENT reports violations and conditions to the District-wide Privacy and Security Official and/or the Agency Privacy Officer of the covered component within the District's Hybrid Entity.

d. RECIPIENT agrees to establish procedures for mitigating, and to mitigate to the extent practicable, any deleterious effects that are known to RECIPIENT of a use or disclosure of PHI by RECIPIENT in violation of the requirements of this DUA.

e. RECIPIENT agrees to report to DHCF, in writing, any use or disclosure of the PHI not permitted or required by this DUA or other incident or condition arising out the Security Rule, including breaches of unsecured PHI as required at 45 C.F.R § 164.410, to the District-wide Privacy and Security Official or agency Privacy Officer within ten (10) business days from the time RECIPIENT becomes aware of such unauthorized use or disclosure. However, if RECIPIENT is a RECIPIENT of the District (i.e., performing delegated essential governmental functions), RECIPIENT must report the incident or condition immediately. Upon the determination of an actual data breach, and in consultation with the District's Privacy and Security Official, RECIPIENT will handle breach notifications to individuals, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), and potentially the media, on behalf of the District.

f. RECIPIENT agrees to ensure that any Workforce member or any agent, including a subcontractor, agrees to the same restrictions and conditions that apply through this DUA with respect to PHI received from RECIPIENT, PHI created by RECIPIENT, or PHI received by RECIPIENT on behalf of DHCF.

g. In accordance with 45 C.F.R §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of RECIPIENT agree to the same restrictions, conditions, and requirements that apply to RECIPIENT with respect to such information.

h. Initially, within ten (10) business days following the commencement of this Agreement, RECIPIENT agrees to provide the District a list of all partner organizations who meet the definition of a business associate. Additionally, RECIPIENT agrees to ensure its partners, including subcontractors, understanding of liability and monitor, where applicable, compliance with the Security Rule and applicable privacy provisions in this DUA.

i. RECIPIENT agrees to provide access within five (5) business days, at the request of DHCF or an Individual, at a mutually agreed upon location, during normal business hours, and in a format as directed by the District Privacy Official or agency Privacy Officer, or as otherwise mandated by the Privacy Rule or applicable District laws, rules and regulations, to PHI in a Designated Record Set, to DHCF or an Individual, to facilitate the District's compliance with the requirements under 45 C.F.R. §164.524.

j. RECIPIENT agrees to make any amendment(s) within five (5) business days to the PHI in a Designated Record Set that DHCF directs or agrees to pursuant to 45 C.F.R § 164.526 in a format as directed by the District Privacy Official or agency Privacy Officer in order to facilitate the District's compliance with the requirements under 45 C.F.R. §164.526.

k. RECIPIENT agrees to use the standard practices of DHCF to verify the identification and authority of an Individual who requests the PHI in a Designated Record Set of a recipient of services from or through DHCF. RECIPIENT agrees to implement policies and procedures to validate the identity of any individual requesting an accounting of disclosures of their PHI.

l. RECIPIENT agrees to record authorizations and log such disclosures of PHI and information related to such disclosures as would be required for DHCF to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and applicable District laws, rules and regulations .

m. RECIPIENT agrees to provide to DHCF or an Individual, within five (5) business days of a request at a mutually agreed upon location, during normal business hours, and in a format designated by the District's Privacy and Security Official or agency Privacy Officer and the duly authorized RECIPIENT Workforce member, information collected in accordance with Paragraph (i) of this Section above, to permit DHCF to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, and applicable District laws, rules and regulations.

n. RECIPIENT agrees to make internal practices, books, and records, including policies and procedures, and PHI, relating to the use and disclosure of PHI received from RECIPIENT, or created, or received by RECIPIENT on behalf of DHCF, available to DHCF, or to the Secretary, within five (5) business days of their request and at a mutually agreed upon location, during normal business hours, and in a format designated by the District Privacy and Security Official or agency Privacy Officer and the duly authorized RECIPIENT Workforce member, or in a time and manner designated by the Secretary, for purposes of the Secretary in determining compliance of DHCF with the Privacy Rule.

o. To the extent RECIPIENT is to carry out one or more of DHCF's obligation(s) under Subpart E of 45 C.F.R Part 164,RECIPIENT agrees to comply with the requirements of Subpart E that apply to DHCF in the performance of such obligation(s).

p. As deemed necessary by the District, RECIPIENT agrees to the monitoring and auditing of items listed in paragraph 2 of this DUA, as well as data systems storing or transmitting PHI, to verify compliance.

q. RECIPIENT may aggregate PHI in its possession with the PHI of other Covered Entities that RECIPIENT has in its possession through its capacity as a Business Associate to other Covered Entities provided that the purpose of the Data Aggregation is to provide DHCF with data analyses to the Health Care Operations of DHCF. Under no circumstances may RECIPIENT disclose PHI of one Covered Entity to another Covered Entity absent the explicit written authorization and consent of the Privacy Officer or a duly authorized Workforce member of DHCF.

r. RECIPIENT may de-identify any and all PHI provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(a)-(b) and any associated HHS guidance. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute PHI and is not subject to the terms of this DUA.

s. All DHCF claims data and derived data products containing DHCF PHI received or created by RECIPIENT shall be maintained on servers and networks in the United States. In the case of cloud-based applications used by RECIPIENT or its subcontractors or agents, RECIPIENT shall stipulate that only US-based servers and networks will used by the cloud-based applications that host, store or analyze DHCF PHI data or derived data products containing PHI.

t. RECIPIENT agrees to not re-identify limited data set information provided as part of this agreement, or contact the individual.

3. Permitted Uses and Disclosures by RECIPIENT

a. Except as otherwise limited in this DUA, RECIPIENT may use or disclose PHI to perform functions, activities, or services for, or on behalf of, DHCF as specified in this Agreement provided that such use or disclosure would not violate Subpart E of 45 C.F.R Part 164 if the same activity were performed by DHCF or would not violate the minimum necessary policies and procedures of DHCF.

b. Except as otherwise limited in this DUA, RECIPIENT may use PHI for the proper management and administration of RECIPIENT or to carry out the legal responsibilities of RECIPIENT.

c. Except as otherwise limited in this DUA, RECIPIENT may disclose PHI for the proper management and administration of RECIPIENT, provided that the disclosures are Required By Law, or RECIPIENT obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used, or further disclosed, only as Required By Law, or for the purpose for which it was disclosed to the person, and the person notifies RECIPIENT of any instances of which it has knowledge that the confidentiality of the information has been breached.

d. Except as otherwise limited in this DUA, RECIPIENT may use PHI to provide Data Aggregation services to DHCF as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

e. RECIPIENT may use PHI to report violations of this DUA or the HIPAA Regulations to the appropriate federal and District of Columbia authorities, consistent with 45 C.F.R. § 164.502(j)(1)-(2).

4. Additional Obligations of RECIPIENT

a. RECIPIENT shall submit a written report to DHCF that identifies the files and reports that constitute the Designated Record Set of DHCF. RECIPIENT shall submit said written report to the Privacy Officer no later than thirty (30) business days after the commencement of this DUA. In the event that RECIPIENT utilizes new files or reports which constitute the Designated Record Set, RECIPIENT shall notify DHCF of said event within thirty (30) days of the commencement of the file's or report's usage. The Designated Record Set file shall include, but not be limited to the identity of the following:

i. Name of the Business Associate of the Covered Entity;

ii. Title of the Report/File;

iii. Confirmation that the Report/File contains PHI(Yes or No);

iv. Description of the basic content of the Report/File;

v. Format of the Report/File (Electronic or Paper);

vi. Physical location of Report/File;

vii. Name and telephone number of current member(s) of the Workforce of DHCF or other District Government agency responsible for receiving and processing requests for PHI; and

viii. Supporting documents if the recipient/personal representative has access to the Report/File.

b. RECIPIENT must provide assurances to DHCF that it will continue to employ sufficient administrative, technical and physical safeguards, as described under the Security Rule, to protect and secure (DHCF's) ePHI entrusted to it. These safeguards include:

i. RECIPIENT agrees to administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that RECIPIENT creates, receives, maintains or transmits on behalf of DHCF.

ii. RECIPIENT agrees to report to DHCF any security incident of which it becomes aware, including any attempts to access ePHI, whether those attempts were successful or not.

iii. This DUA may be terminated if DHCF determines that RECIPIENT has materially breached the agreement.

iv. RECIPIENT agrees to make all policies and procedures, and documents relating to security, available to the Secretary of HHS for the purposes of determining DHCF's compliance with HIPAA.

v. This DUA continues in force for as long as RECIPIENT retains any access to DHCF's ePHI.

vi. With respect to the subset of PHI known as electronic PHI (ePHI) as defined by HIPAA Security Standards at 45 C.F.R. §§ 160 and 164, subparts A and C (the "Security Rule"), if in performing the Services, RECIPIENT, its employees, agents, subcontractors and any other individual permitted by RECIPIENT will have access to any computer system, network, file, data or software owned by or licensed to Provider that contains ePHI, or if RECIPIENT otherwise creates, maintains, or transmits ePHI on Provider's behalf, RECIPIENT shall take reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software. With respect to the security of ePHI, RECIPIENT shall: (a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Provider; (b) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (c) Report to the Provider any security incident of which it becomes aware.

vii. RECIPIENT agrees not to electronically transmit or permit access to PHI unless such transmission or access is authorized by this DUA and further agrees that it shall only transmit or permit such access if such information is secured in a manner that is consistent with applicable law, including the Security Rule. For purposes of this DUA "encrypted" shall mean the reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form. If DHCF stores, uses or maintains PHI in encrypted form, or in any other secured form acceptable under the security regulations, DHCF shall promptly, at request, provide with the key or keys to decrypt such information and will otherwise assure that such PHI is accessible upon reasonable request.

viii. In the event RECIPIENT performs functions or activities involving the use or disclosure of PHI on behalf of Covered Entity that involve the installation or maintenance of any software (as it functions alone or in combination with any hardware or other software),RECIPIENT shall ensure that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform of any software standards or specifications not compliant with the HIPAA Regulations.

c. At the request of DHCF, RECIPIENT agrees to amend this DUA to comply with all HIPAA mandates.

d. Upon completion of the analysis, RECIPIENT agrees to provide a draft copy of the report to DHCF for purposes of review and comment. DHCF will have thirty (30) days to review and comment from receipt of the draft report.

5. Sanctions

RECIPIENT agrees that its Workforce members, agents and subcontractors who violate the provisions of HIPAA or other applicable federal or District privacy law will be subject to discipline in accordance with Business Associate's internal Personnel Policy and applicable collective bargaining agreements. RECIPIENT agrees to impose sanctions consistent with RECIPIENT's personnel policies and procedures and applicable collective bargaining agreements with respect to persons employed by it. Members of RECIPIENT's Workforce who are not employed by RECIPIENT are subject to the policies and applicable sanctions for violation of this DUA In the event RECIPIENT imposes sanctions against any member of its Workforce, agents and subcontractors for violation of the provisions of HIPAA or other applicable federal or District privacy laws, RECIPIENT shall inform the District Privacy Official or the agency Privacy Officer/Liaison of the imposition of sanctions.

6. Obligations of DHCF

a. DHCF shall notify RECIPIENT of any limitation(s) in its Notice of Privacy Practices of DHCF in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect the use or disclosure of PHI by RECIPIENT.

b. DHCF shall notify RECIPIENT of any changes in, or revocation of, permission by the Individual to the use or disclosure of PHI, to the extent that such changes may affect the use or disclosure of PHI by RECIPIENT.

c. DHCF shall notify RECIPIENT of any restriction to the use or disclosure of PHI that DHCF has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the use or disclosure of PHI by RECIPIENT.

7. Permissible Requests by DHCF

DHCF shall not request RECIPIENT to use or disclose PHI in any manner that would not be permissible under the Privacy Rule and Subpart E of 45 C.F.R Part 164 if done by DHCF.

8. Representations and Warranties.

RECIPIENT represents and warrants to DHCF:

a. That it is duly organized, validly existing, and in good standing under the laws of the jurisdiction in which it is organized or licensed, it has the full power to execute this DUA and it, its employees, agents, subcontractors, representatives and members of its Workforce are licensed and in good standing with the applicable agency, board, or governing body to perform its obligations hereunder, and that the performance by it of its obligations under this DUA has been duly authorized by all necessary corporate or other actions and will not violate any provision of any license, corporate charter or bylaws;

b. That it, its employees, agents, subcontractors, representatives and members of its Workforce are in good standing with the District, that it, its employees, agents, subcontractors, representatives and members of its Workforce will submit a letter of good standing from the District, and that it, its employees, agents, subcontractors, representatives and members of its Workforce have not been de-barred from being employed as a contractor by the federal government or District;

c. That neither the execution of this DUA, nor its performance hereunder, will directly or indirectly violate or interfere with the terms of another agreement to which it is a party, or give any governmental entity the right to suspend, terminate, or modify any of its governmental authorizations or assets required for its performance hereunder. RECIPIENT represents and warrants to DHCF that it will not enter into any agreement the execution or performance of which would violate or interfere with this DUA;

d. That it is not currently the subject of a voluntary or involuntary petition in bankruptcy, does not currently contemplate filing any such voluntary petition, and is not aware of any claim for the filing of an involuntary petition;

e. That all of its employees, agents, subcontractors, representatives and members of its Workforce, whose services may be used to fulfill obligations under this DUA are or shall be appropriately informed of the terms of this DUA and are under legal obligation to RECIPIENT, by contract or otherwise, sufficient to enable RECIPIENT to fully comply with all provisions of this DUA. Modifications or limitations that DHCF has agreed to adhere to with regards to the use and disclosure of PHI of any individual that materially affects or limits the uses and disclosures that are otherwise permitted under the Privacy Rule will be communicated to RECIPIENT, in writing, and in a timely fashion;

f. That it will reasonably cooperate with DHCF in the performance of the mutual obligations under this Agreement;

g. That neither RECIPIENT, nor its shareholders, members, directors, officers, agents, subcontractors, employees or members of its Workforce have been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or District healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or District law (including without limitation following a plea of *nolo contendere* or no contest or participation in a first offender deferred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item

or service, under a federal or District healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in part by any federal, state, or local government agency (d) the unlawful, manufacture, distribution, prescription or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. RECIPIENT further agrees to notify DHCF immediately after RECIPIENT becomes aware that any of the foregoing representations and warranties may be inaccurate or may become incorrect.

9. Term and Termination

a. *Term.* The requirements of this DUA shall be effective as of the date of the execution of this Agreement, and shall terminate on the earlier of the two dates:

   i. Twelve (12) months from the date of the execution of the Agreement; or

   ii. When all of the PHI provided by DHCF to RECIPIENT, or created or received by RECIPIENT on behalf of DHCF, is confidentially destroyed or returned to DHCF within five (5) business days of its request, the PHI shall be returned in a format mutually agreed upon by and between the Privacy Official and/or Privacy Officer or their designee and the appropriate and duly authorized Workforce member of RECIPIENT. If it is infeasible to return or confidentially destroy the PHI, protections shall be extended to such information, in accordance with the termination provisions in this Section and communicated to the Privacy Official or Privacy Officer or their designee. The requirement to return PHI to the District at the end of this Agreement term or if the Agreement is terminated applies irrespective of whether RECIPIENT is also a Covered Entity under HIPAA.

b. *Option to Extend*. Prior to the expiration of the term of the Agreement, both parties may agree to modify the Agreement to extend the Term by a period of 12 months. This agreement may occur up to four (4) times and the maximum Term of this Agreement shall not exceed sixty (60) months.

c. *Termination for Cause.* Upon DHCF's knowledge of a material breach of this DUA by RECIPIENT, DHCF shall either:

   i. Provide an opportunity for RECIPIENT to cure the breach within a period of ten (10) days (or such longer period as the District may authorize in writing) after receipt of notice from the Privacy Officer specifying such failure or end the violation and terminate this Agreement if RECIPIENT does not cure the breach or end the violation within the time specified by DHCF; or

   ii. Immediately terminate this Agreement if RECIPIENT breaches a material term of this DUA and a cure is not possible.

   If neither termination nor cure is feasible, DHCF shall report the violation to the Secretary of HHS.

d. *Effect of Termination.*

i. Upon termination of this Agreement, for any reason, RECIPIENT shall return in **a mutually agreed upon format or confidentially destroy** all PHI received from DHCF, or created or received by RECIPIENT on behalf of DHCF within five (5) business days of termination. This provision shall apply to PHI that is in the possession of ALL subcontractors, agents or Workforce members of RECIPIENT. RECIPIENT shall retain no copies of PHI in any form.

ii. In the event that RECIPIENT determines that returning or destroying the PHI is infeasible, RECIPIENT shall provide written notification to DHCF of the conditions that make the return or confidential destruction infeasible. Upon determination by the agency Privacy Officer/Liaison that the return or confidential destruction of the PHI is infeasible, RECIPIENT shall extend the protections of this DUA to such PHI and limit further uses and disclosures of such PHI for so long as RECIPIENT maintains such PHI. Additionally, RECIPIENT shall:

(1) Retain only that PHI which is necessary for RECIPIENT to continue its proper management and administration or to carry out its legal responsibilities;

(2) Return to DHCF [or, if agreed to by DHCF, destroy] the remaining PHI that RECIPIENT still maintains in any form;

(3) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R Part 164 with respect to ePHI to prevent use or disclosure of the PHI, other than as provided for in this section, for as long as RECIPIENT retains the PHI;

(4) Not use or disclose the PHI retained by RECIPIENT other than for the purposes for which such PHI was retained and subject to the same conditions set out in Section 3. Permitted Uses and Disclosures by the Business Associate, which applied prior to termination; and

(5) Return to DHCF [or, if agreed to by DHCF, destroy] the Protected Health Information retained by RECIPIENT when it is no longer needed by RECIPIENT for its proper management and administration or to carry out its legal responsibilities.

The obligations outlined in Section 2. Obligations and Activities of RECIPIENT shall survive the termination of this Agreement.

10. Miscellaneous

a. *Regulatory References.* A reference in this DUA to a section in the Privacy Rule means the section as in effect or as amended.

b. *Amendments.* DHCF and RECIPIENT ("the Parties") agree to take such action as is necessary to amend this DUA from time to time

i. As is necessary for DHCF to comply with the requirements of the Privacy Rule and HIPAA Regulations. Except for provisions Required By Law as defined herein, no provision hereof shall be deemed waived unless in expressed in writing

and signed by duly authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy under this DUA; or

ii. To update the requested data elements, time frame, study title or other programmatic considerations outlined in this DUA, provided the specified a) data type and b) scope of work are consistent with the signed Agreement. Such amendments must be dated and initialed in Appendix A by duly authorized representatives of the Parties. All other requests shall require the creation of a new DUA.

c. *Interpretation.* Any ambiguity in this DUA shall be resolved to permit compliance with applicable federal and District laws, rules and regulations, and the HIPAA Rules, and any requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary; provided that applicable federal and District laws, rules and regulations shall supersede the Privacy Rule if, and to the extent that they impose additional requirements, have requirements that are more stringent than or provide greater protection of patient privacy or the security or safeguarding of PHI than those of the HIPAA Regulations.

d. *Third-Party Beneficiaries*. DHCF and RECIPIENT are the only parties to this DUA and are the only parties entitled to enforce its terms. Except for the rights of Individuals, as defined herein, to have access to and amend their PHI, and to an accounting of the uses and disclosures thereof, in accordance with paragraphs (2)(f), (g) and (j) of this DUA, nothing in the DUA gives, is intended to give, or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons.

e. *Compliance with Applicable Law*. RECIPIENT shall comply with all federal and District laws, regulations, executive orders and ordinances, as they may be amended from time to time during the term of this DUA to the extent they are applicable to this DUA.

f. *Governing Law and Forum Selection*. This DUA shall be construed broadly to implement and comply with the requirements relating to the Privacy Rule, and other applicable laws and regulations. All other aspects of this DUA shall be governed under the laws of the District. DHCF and RECIPIENT agree that all disputes which cannot be amicably resolved by DHCF and RECIPIENT regarding this DUA shall be litigated before the Superior Court of the District of Columbia, the District of Columbia Court of Appeals, or the United States District Court for the District of Columbia having jurisdiction, as the case may be. DHCF and RECIPIENT expressly waive any and all rights to initiate litigation, arbitration, mediation, negotiations and/or similar proceedings outside the physical boundaries of the District of Columbia and expressly consent to the jurisdiction of the above tribunals.

g. *Indemnification*. RECIPIENT shall indemnify, hold harmless and defend DHCF from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking of RECIPIENT under this DUA; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with the performance of RECIPIENT under this DUA.

h. *Injunctive Relief*. Notwithstanding any rights or remedies under this DUA or provided by law, DHCF retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by RECIPIENT, its Workforce, any of its subcontractors, agents, or any third party who has received PHI from RECIPIENT.

i. *Assistance in litigation or administrative proceedings*. RECIPIENT shall make itself and any agents, affiliates, subsidiaries, subcontractors or its Workforce assisting RECIPIENT in the fulfillment of its obligations under this DUA, available to DHCF, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCF, its directors, officers or employees based upon claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where RECIPIENT or its agents, affiliates, subsidiaries, subcontractors or its Workforce are a named adverse party.

j. *Notices.* Any notices between the Parties or notices to be given under this DUA shall be given in writing and delivered by personal courier delivery or overnight courier delivery, or by certified mail with return receipt requested, to RECIPIENT or to DHCF, to the addresses given for each Party below or to the address either Party hereafter gives to the other Party. Any notice, being addressed and mailed in the foregoing manner, shall be deemed given five (5) business days after mailing. Any notice delivered by personal courier delivery or overnight courier delivery shall be deemed given upon notice upon receipt.

If to _____, to	If to DHCF, to
_____	441 4th St., NW, Suite 900S
_____	Washington, DC 20001
Attention: Privacy Officer	Attention: Cecelia Davis, Privacy Officer
Fax:_____	Fax: (202) 442-9053

k. *Headings*. Headings are for convenience only and form no part of this DUA and shall not affect its interpretation.

l. *Counterparts; Facsimiles*. This DUA may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

m. *Successors and Assigns*. The provisions of this DUA shall be binding upon and shall inure to the benefit of the Parties hereto and their respective successors and permitted assigns, if any.

n. *Severance*. In the event that any provision of this DUA is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this DUA will remain in full force and effect. In addition, in the event a Party believes in good faith that any provision of this DUA fails to comply with the then-current requirements of the Privacy Rule, such party shall notify the other Party in writing, in the manner set forth in Section 10. Miscellaneous, Paragraph j. Notices. Within ten (10) business days from receipt of notice, the Parties shall address in good faith such concern and amend the terms of this DUA, if necessary to bring the contested provision(s) into compliance.

o. *Entire Agreement*. This DUA, as may be amended from time to time pursuant to Section 10. Miscellaneous, Paragraph b. Amendment, which incorporates by reference this Agreement, constitutes the entire agreement and understanding between the Parties and supersedes all prior oral and written agreements and understandings between them with respect to applicable District and federal laws, rules and regulations, HIPAA and the Privacy Rule, and any rules, regulations,

requirements, rulings, interpretations, procedures, or other actions related thereto that are promulgated, issued or taken by or on behalf of the Secretary of HHS.

SIGNED this _____day of_____, 20__.

_____ (insert organization name)

BY: _____

_____ (insert authorized representative's name)

_____ (insert title of organization's authorized representative)

SIGNED this _____day of_____, 20__.

DEPARTMENT OF HEALTH CARE FINANCE

BY: _____

_____ (insert authorized representative's name)

_____ (insert title of organization's authorized representative)

APPENDIX A – Requested Data Elements for [ ] Project

DC Medicaid Data Request

Data Element or Field	**Data Table** (if known)	**Intended Use**	**Priority** (high, med, low)	**Comments**

Instructions:

Please provide a description of the requested data elements, their intended use and the priority you assign to each data element. If you know the data table that contains the requested data field(s) you may provide those instead. If there are any needed comments for data formatting or methodological considerations, please use the comments column. You may modify the table to add additional rows as needed.

APPENDIX B – List of Modifications to DUA Language for [ ] Project

Data Use Agreement Category

- ☐ **De-identified Data**
- ☐ **Limited Data Set**
- ☐ **Masked or Pseudo-anonymized Data Set**

Original Section	Proposed Modification	Rationale	

Definitions:

De-identified Data Set – *A data set that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual; does not contain individually identifiable health information as referenced in 45 CFR 164.514 (b)(2)(i).*

Limited Data Set – *A limited data set is protected health information that excludes sixteen specific direct identifiers of the individual or of relatives, employers, or household members of the individual as listed in 45 CFR 164.514 (e)(2)(i-xvi).*

Masked or Pseudo-anonymized Data Set – *A data set that replaces fields containing individually identifiable health information within a database with artificial identifiers, or pseudonyms. For example, a name is replaced with a unique number.*

NOTE: If the Recipient's operational definitions differ substantially from the above definitions, please contact the DHCF Information & Privacy Officer and the Data Officer to explain.