

**DATA USE AGREEMENT BETWEEN THE  
MARYLAND HEALTH CARE COMMISSION AND  
BALTIMORE CITY LAW DEPARTMENT**

This Data Use Agreement (“Agreement”) is made by and between the Maryland Health Care Commission (“MHCC”), located at 4160 Patterson Avenue, Baltimore, Maryland 21215, and Baltimore City Law Department (the “Data Recipient”) located at C/O City Hall, Room 101, 100 N. Holliday Street, Baltimore, Maryland 21209 (each a “Party” and, collectively, the “Parties”), to govern the release, use, privacy and security of Maryland Medical Care Data Base (“MCDB”) data provided by MHCC to the Data Recipient.

**WHEREAS**, under §§19-103(c)(3) and (4) and 19-133 of the Health-General Article of the Annotated Code of Maryland, and COMAR 10.25.06, MHCC is authorized to collect and store, *inter alia*, health care claims data for Maryland residents enrolled in commercial insurance, Medicare and the Medicaid Assistance Program (“Medicaid”) managed care organizations, and non-Maryland residents enrolled in Maryland commercial insurance plans, in the MCDB;

**WHEREAS**, the Data Recipient, by written application dated August 29, 2022, submitted to MHCC, requested access to the following data sets:

MCDB commercial claims data files for calendar years 2010 - 2020 and Medicaid data claims files for calendar years 2011- 2020 for a project entitled, *Assessing Extent of Opioid Epidemic in Baltimore City*

**WHEREAS**, the MCDB data is patient-specific data containing both protected health information (“PHI”) and personally identifiable information (“PII”), including unique patient identification numbers (encrypted), partial dates of birth, sex of patient, zip code of residence, provider identification numbers, diagnosis codes, dates of service, and insurer plan and type of product information; thus, MHCC and the Data Recipient consider the security and confidentiality of this data to be a matter of high priority.

**NOW THEREFORE**, in consideration of the mutual promises and covenants, the sufficiency of which is hereby acknowledged, MHCC and the Data Recipient agree as follows:

**AGREEMENT**

The above recitals and following attachments are fully incorporated into this Agreement:

- Attachment A – Covered Data;
- Attachment B – Scope of Work and Project Methodology
- Attachment C – Additional Data Sources
- Attachment D – Data Users Log;
- Attachment E – Data Management Plan and Data Storage Location; and
- Attachment F – Certificate of Data Destruction.

## **1. DATA TO BE RELEASED**

1.1 MHCC will provide to Data Recipient the electronic files described in Attachment A (“Covered Data”).

1.2 The Covered Data files will have a “SAS7BDAT” extension. MHCC will send the Covered Data to Data Recipient via a SSH File Transport Protocol (SFTP). Data Recipient agrees to set up an appropriate location to download the Covered Data in compliance with this Agreement and the Data Management Plan contained in Attachment E (“Data Management Plan and Data Storage Location”).

1.3 Data Recipient agrees that MHCC shall retain all ownership rights to the Covered Data provided to Data Recipient and that Data Recipient does not obtain any right, title, or interest in any of the data provided by MHCC.

## **2. PERMITTED USES OF THE COVERED DATA**

2.1 The Covered Data shall be used solely to support the project entitled “Assessing Extent of Opioid Epidemic in Baltimore City” as described in Attachment B (“Scope of Work”). Any other uses of the Covered Data outside of the Scope of Work described in Attachment B are strictly prohibited unless prior written approval is obtained from MHCC.

2.1.1 Data Recipient in its application states a plan to use the Covered Data as follows:

The opioid epidemic is the worst drug epidemic in our nation's history. In 2019, an estimated 49,860 people died in the U.S. from opioids, more than those who died from motor vehicle accidents, suicide, gun violence, or at the peak of the AIDS epidemic.<sup>1</sup> Though Maryland ranks fifth in opioid-related overdose death rates nationally, the City of Baltimore faces a higher rate of overdoses compared to other areas in Maryland. The number of opioid-related deaths in the City of Baltimore has increased since 2010, reaching 692 deaths in 2017.<sup>2</sup> More recent Baltimore City data from the State of Maryland reports 851 opioid-related deaths in 2019 and 952 opioid-related deaths in 2020.<sup>3</sup> Combating the opioid epidemic has proven difficult for public health officials and other stakeholders for many reasons, including the multitude of contributing factors and downstream effects on individuals and communities. Estimating the burden of the opioid epidemic by epidemiologic methods can be helpful to policymakers to inform and address the needs of individuals affected by the epidemic. Efficient and informed allocation of resources will improve health and reduce long-term costs

associated with combating the opioid epidemic. Useful estimates of burden of the opioid epidemic depend on robust and reliable inputs and should incorporate, whenever possible, information specific to the context in which they are applied. Therefore, data from the MCDB can provide important inputs for location-specific estimates of the opioid epidemic in the City of Baltimore over time. Our findings will provide information to stakeholders seeking to abate the opioid epidemic in the City of Baltimore. The data are sought solely for litigation purposes.

1. Centers for Disease Control and Prevention (CDC). “Drug Overdose Deaths.” [https://www.cdc.gov/drugoverdose/data/statedeaths.html]
2. Baltimore City Health Department. “Baltimore City’s Response to the Opioid Epidemic.” [https://health.baltimorecity.gov/opioid-overdose/baltimore-city-overdose-prevention-and-response-information]
3. Maryland Opioid Operational Command Center. “2020 Annual Report.” [https://s3.documentcloud.org/documents/20614236/2020-annual-report-final.pdf]

Projects that include dissemination of the data through published studies or other public release must be submitted to MHCC for review prior to publication. Other conditions include:

The Data Recipient may use the Covered Data to develop a report in which the Data Recipient calculates the harms that the opioid epidemic has inflicted on the City of Baltimore. Any report that is publicly filed or otherwise available to the public will only include aggregated, non-identifiable data and will comply with all other requirements of this section.

2.2 Data Recipient may retain the Covered Data and utilize such data for the specific purposes described in Attachment B during the effective dates of this Agreement.

2.3 Data Recipient agrees to provide a list of any files from sources other than the Covered Data that it plans to use in conjunction with the Covered Data in its analysis. Attachment C (“Additional Data Sources”) contains all additional data sources known to Data Recipient at the time of execution of this Agreement. Data Recipient shall update this list, and provide such update to MHCC, prior to the use of any new data source(s) in conjunction with the Covered Data. Data Recipient further agrees not to link member-level data to any additional data source.

2.4 Data Recipient agrees that any use of the Covered Data in the creation of any document (report, study, manuscript, table, chart, etc.) must adhere to MHCC’s cell size suppression policy unless MHCC approves the use of an alternate cell size. This policy requires that no cell of ten (10) or less may be displayed and that no use of percentages or other mathematical formulas may be used if they are based on a sample of ten (10) or fewer patients.

2.5 Data Recipient agrees not to disclose direct findings, listings, or information derived from the Covered Data, with or without direct identifiers, if such findings, listings, or information can,

by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, geographic location, age (if > 89), sex, diagnosis and procedure, admission/discharge date(s), or date of death.

2.6 Data Recipient agrees not to attempt to re-identify individuals whose information is contained in the Covered Data. Data Recipient further agrees to not attempt to link any Covered Data to any other source of clinical or health service information.

### **3. PERMITTED USERS OF THE COVERED DATA**

3.1 The Data Recipient shall limit access to the Covered Data, the Covered Data documentation, and any files derived from the Covered Data to the minimum number of individuals necessary, as determined within the sole discretion of Data Recipient to achieve the purposes set out in Attachment B, and access to the data shall be granted with minimal access and risk to PHI, in accordance with the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, and the implementing regulations at 45 CFR Parts 160 and 164, specifically, 42 CFR § 164.512.

3.2 Data Recipient shall keep a log of the identity of each individual ("Data User") who is authorized to access the data provided under this Agreement. Attachment D ("Data Users Log") contains the log of authorized Data Users known to Data Recipient at the time of execution of this Agreement. After execution of this Agreement, Data Recipient will provide updates of the log to MHCC before authorizing any new individual to access the Covered Data.

3.3 Data Recipient shall be responsible for making all individuals who are permitted Data Users of the Covered Data under this Agreement, including any personnel of contractors and subcontractors, aware of the terms and conditions of this Agreement. Specifically, Data Recipient shall advise all Data Users of the confidential nature of the Covered Data and the safeguards required to protect the security of the data. In addition, Data Recipient shall provide a copy of this Agreement to all Data Users, inform them that they are required to comply with all terms and conditions of this Agreement, and obtain written acknowledgments from each Data User. Data Recipient shall provide documentation of Data Users' written acknowledgments to MHCC upon request.

### **4. DATA SECURITY, CONFIDENTIALITY, AND INSTITUTIONAL REVIEW BOARD APPROVAL**

4.1. Data Recipient agrees to comply with any applicable State and federal security requirements regarding collection, maintenance, and use of the Covered Data, including HIPAA and the implementing regulations at 45 CFR Parts 160 and 164, and the Maryland Confidentiality of Medical Records Act ("MCMRA"), Md. Code Ann., Health-Gen §§ 4-301 *et seq.*

4.2. Data Recipient secured the required Institutional Review Board (IRB) review, in compliance with COMAR 10.25.11, for use of the Covered Data for the project as evidenced by a written exemption document with the subject "IRB Exemption-Regulatory Opinion," dated

October 11, 2021, that was issued by WCG IRB (formerly Western Institutional Review Board (WIRB)). WCG IRB determined that the project was exempt under 45 CFR §46.104(d)(4). The written exemption document indicates that WCG IRB does not impose an expiration date on its exemption determinations.

4.3. The Covered Data is confidential and shall not be disclosed or transferred without written consent of MHCC to anyone or entity other than the authorized dData Users listed in Attachment D (“Data Users Log”).

4.4. Data Recipient will maintain the electronic security of the Covered Data in accordance with the Data Management Plan (“DMP”) submitted by Data Recipient (Attachment E) for each data custodian. Each DMP, which shall be consistent with the [State of Maryland Information Security Policy](#), and relevant State and federal laws, must be approved by MHCC prior to the release of data to Data Recipient.

4.4.1. The Covered Data shall be stored and processed so as to protect the confidentiality of the data, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. If the Covered Data is stored in a folder on a network drive, that folder shall be omitted from the standard data back-up process utilized by Data Recipient. If the Covered Data is stored on a local hard drive, that computer must be in a secure location at all times.

4.4.2. Data Recipient will submit a revised DMP (Attachment E) to MHCC if there are any changes to the plan, including, but not limited to, storage location (in which case a revised Data Storage Location form must also be submitted) and security protocols. MHCC must review and approve any revised DMP (and Data Storage Location, if applicable) before such plan is implemented.

4.5. At the termination of this Agreement for any reason, Data Recipient agrees to destroy the Covered Data, any products created from the Covered Data, and all back-up and archived copies of the Covered Data. The destruction process shall ensure that the data is erased from all networks, drives or computers and could involve using software such as WipeDrive that is capable of destroying data on a drive in a manner that meets the data destruction standards specified by the [National Institute of Standards and Technology \("NIST"\) Special Publication 800-88, Guidelines for Media Sanitation](#). Data Recipient will send a fully executed Certificate of Data Destruction (Attachment F) within thirty (30) days of the date of the termination of this Agreement to MHCC in accordance with section 8 of this Agreement.

4.6. The Parties agree to work together in a mutually agreeable fashion to address technical issues that may arise during project implementation and thereafter. Each Party also agrees to notify the other Party as soon as reasonably practicable if a significant technical issue arises.

## **5. REPORTING AND NOTIFICATION REQUIREMENTS**

5.1. Data Recipient shall submit a semi-annual report to MHCC in the form and manner specified by MHCC, which shall include, but not be limited to, a description of the work performed and uses of the Covered Data; approved changes or expansions to the Scope of Work; approved changes to permitted Data Users; approved changes to data access and security methods; and any approved revisions to the data custodian's data management plan; and a summary of analyses, results, reports, publications, or any other work product derived in whole or part from use of the Covered Data.

5.2. Data Recipient agrees to notify MHCC in writing within 24 hours of receiving a request, subpoena, or order for disclosure relating to the Covered Data, whether for a judicial proceeding or matter, an administrative hearing, a request under Maryland's Public Information Act ("PIA") or the federal Freedom of Information Act ("FOIA"), or similar request. Data Recipient shall not disclose the Covered Data without either prior MHCC's written agreement or before affording the MHCC sufficient time to intervene in opposition to such a request, subpoena, or order.

## **6. BREACH OF AGREEMENT**

6.1 Data Recipient shall give MHCC written notice immediately or as soon as reasonably practicable upon having reason to know that a potential or actual Data Breach, as defined in Section 6.2, has occurred.

6.2 "Data Breach" means the unauthorized acquisition, access, use, or disclosure of the Covered Data, or any unsecured PHI that compromises the security or privacy of such information, subject to the statutory exceptions specified at Section 13400 of the Health Information Technology for Economic Clinical Health Act ("HITECH Act") and the regulatory exclusions specified at 45 CFR §164.402 and any future amendments thereto.

6.3 Any breach of security or unauthorized use or disclosure of the Covered Data, including a Data Breach, shall constitute a breach of this Agreement. Any violation of State or federal law with respect to disclosure of the Covered Data, including but not limited to, the MCMRA or the HIPAA Privacy Rule, shall constitute a breach of this Agreement. Notwithstanding the breaches specifically enumerated above, any other failure by Data Recipient to comply with the terms and obligations of this Agreement shall constitute a breach of this Agreement.

6.4 Any alleged failure of MHCC to act upon a notice of a breach of this Agreement does not constitute a waiver of such breach, nor does it constitute a waiver of any subsequent breach(es).

6.5 The Data Recipient shall comply and assist in any audit of compliance with this Agreement if requested by MHCC. In the event that MHCC reasonably believes that the confidentiality of the Covered Data has been breached, MHCC may: investigate the matter, including an on-site inspection for which Data Recipient shall provide access; and require Data Recipient to develop a written plan of correction, acceptable to MHCC, to ameliorate or minimize the damage caused by the breach of confidentiality and to prevent future breaches of data confidentiality.

6.6 In the event of a breach of this Agreement, MHCC may seek all other appropriate remedies available under law, including termination of this Agreement, disqualification of Data Recipient from receiving PHI or PII from MHCC in the future, and referral of any inappropriate use or disclosure to the Consumer Protection Division of the Office of the Attorney General of Maryland, the Maryland State’s Attorney Office, or any other appropriate state or federal law enforcement authority.

**7. FEES**

7.1 Data Recipient agrees to pay to MHCC a one-time fee in the amount \$162,000 for the Covered Data, consisting of ten (10) years of data for Medicaid (2011 – 2020) and eleven (11) years of data for Commercial files (2010 – 2020).

Data Recipient shall pay the one-time fee of \$162,000 in full to MHCC before any of the Covered Data is provided to Data Recipient.

<b>Commercial Data File Cost for years 2010 - 2020 for all files namely eligibility file, professional services file, institutional services file, and pharmacy file</b>		<b>Rate</b>	<b>Year of Data Requested</b>	<b>Total Cost</b>
<b>Years</b>	<b>Tier</b>		<b>Total</b>	<b>\$84,000</b>
				<b>Cost for all four data files</b>
1	Tier One	100%	2020	\$12,000
2	Tier One	100%	2019	\$12,000
3	Tier Two	75%	2018	\$9,000
4	Tier Two	75%	2017	\$9,000
5	Tier Three	50%	2016	\$6,000
6	Tier Three	50%	2015	\$6,000
7	Tier Three	50%	2014	\$6,000
8	Tier Three	50%	2013	\$6,000
9	Tier Three	50%	2012	\$6,000
10	Tier Three	50%	2011	\$6,000
11	Tier Three	50%	2010	\$6,000

<b>Medicaid Data File Cost for years 2011 - 2020 for all files namely eligibility file, professional services file, institutional services file, and pharmacy file</b>		<b>Rate</b>	<b>Year of Data Requested</b>	<b>Total Cost</b>
<b>Years</b>	<b>Tier</b>		<b>Total</b>	<b>\$78,000</b>
				<b>Cost for all four data files</b>
1	Tier One	100%	2020	\$12,000
2	Tier One	100%	2019	\$12,000
3	Tier Two	75%	2018	\$9,000
4	Tier Two	75%	2017	\$9,000
5	Tier Three	50%	2016	\$6,000

6	Tier Three	50%	2015	\$6,000
7	Tier Three	50%	2014	\$6,000
8	Tier Three	50%	2013	\$6,000
9	Tier Three	50%	2012	\$6,000
10	Tier Three	50%	2011	\$6,000

7.2 No reimbursement will be made to either Party by the other Party for expenses related to accessing, maintaining, or upgrading a Party's information technology infrastructure, or for any expenses related to extracting, using, or storing the Covered Data, or for any other expense otherwise arising out of this Agreement.

## 8. NOTICE

Any notice given pursuant to this Agreement must be in writing and addressed to:

If to MHCC:

Mahlet Nigatu,  
Chief of APCD Public Report and Data Release  
Maryland Health Care Commission  
4160 Patterson Ave.  
Baltimore, MD 21215  
[Mahlet.Nigatu@maryland.gov](mailto:Mahlet.Nigatu@maryland.gov)  
(410)-764-3779

If to Data Recipient:

Sara Gross, JD  
Chief Solicitor  
Baltimore City Law Department  
C/O City Hall, Room 101, 100 N. Holliday Street  
Baltimore, MD, 21209  
[Sara.gross@baltimorecity.gov](mailto:Sara.gross@baltimorecity.gov)  
(410)-396-3297

## 9. GOVERNING LAW AND JURISDICTION

This Agreement shall be construed, interpreted, and enforced according to the laws of the State of Maryland without reference to its conflict of laws principles. Data Recipient acknowledges doing business in Maryland and agrees to submit to the jurisdiction of the courts in Maryland in the event of an action for an alleged breach of this Agreement.

## 10. EFFECTIVE DATE, AMENDMENTS, MODIFICATIONS, AND TERMINATION

10.1 This Agreement becomes effective on the date of its execution and shall remain in effect until 12/31/2023 from the date this Agreement is executed, or upon termination of the Agreement by either Party in accordance with section 10.3 below.

10.2 This Agreement may be amended or modified if mutually agreed to in writing by the Parties.

10.3 This Agreement may be terminated by either Party, with or without cause, provided that written notice is given to the non-terminating Party at least thirty (30) days before the determined termination date.

**In acknowledgment of the foregoing, the Parties by their duly authorized officials do hereby indicate their consent to this Data Use Agreement.**

Maryland Health Care Commission

Data Recipient Name

Signed:

Signed:

\_\_\_\_\_  
Ben Steffen

\_\_\_\_\_  
Printed Name:

Executive Director

Title

Date:

Date:

## ATTACHMENT A – Covered Data

This Data Use Agreement pertains to the following MCDB claims data files for the calendar years listed below:

<b>Data Types /Years</b>	<b>Pharmacy Claims Files</b>	<b>Eligibility Claims Files</b>	<b>Professional Health Claims Files</b>	<b>Institutional Claims Files</b>
2010	Commercial	Commercial	Commercial	Commercial
2011	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2012	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2013	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2014	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2015	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2016	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2017	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2018	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2019	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid
2020	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid	Commercial/Medicaid

**ATTACHMENT B – Scope of Work and Project Methodology**

ATTACHMENT A: SCOPE OF WORK FROM THE APPLICATION WILL BE INSERTED HERE.

DRAFT

**ATTACHMENT C – Additional Data Sources**

No additional data sources required

DRAFT





DRAFT

**ATTACHMENT E – Data Management Plans and Data Storage Locations**

**ATTACHMENT E1 from the Application will be inserted here.**

DRAFT

**Attachment F: Certificate of Data Destruction**

**Maryland Health Care Commission (MHCC) Medical Claims Database  
CERTIFICATE OF DATA DESTRUCTION**

Data must be destroyed so that it cannot be recovered from electronic storage media in accordance with the methods established by the “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,” as established by the U.S. Department of Health and Human Services (HHS).

The undersigned hereby certifies that all copies of the following data files provided to the **Data Recipient Name** have been destroyed.

<b>Project Title</b>	
<b>MHCC DUA Number</b>	
<b>Principal Investigator Name</b>	
Title	
Organization	
Address	
Tel Number	
Fax Number:	
E-mail Address	
<b>Data Custodian Name</b>	
Title	
Organization	
Address	
Tel Number	
Fax Number	
E-mail Address	
<b>Date the Data was Destroyed:</b>	

**Description of files provided:**

	<b>Data Files Provided Under Referenced DUA</b>
Pharmacy Claims Files	
Eligibility Claims Files	
Professional Health Claims Files	
Institutional Claims Files	

Describe how the Data Custodian, System Owner/Maintainer has disposed of, destroyed, erased, and/or anonymized the file regardless of the method of storage. Use as much space as needed to provide a complete description.

[Add description here:](#) (fillable field)

**Certification**

I/we certify that we have destroyed all Data received from MHCC in connection with this project, in all media that were used during the research project. This includes, but is not limited to data maintained on hard drive(s), diskettes, CDs, etc.

**SIGNATURES:**

<b>Principal Investigator</b>	<b>Data Custodian</b>
Organization: _____	Organization: _____
Signature _____	Signature _____
Printed Name _____	Printed Name _____
Title _____	Title _____
Date _____	Date _____
<b>Person Responsible for Destroying the Data</b>	<b>Signature Witness</b>
Organization _____	Organization _____
Signature _____	Signature _____
Printed Name _____	Printed Name _____
Title _____	Title _____
Date _____	Date _____