

## DATA USE AGREEMENT

### BETWEEN THE

### MARYLAND HEALTH CARE COMMISSION AND

### JOHNS HOPKINS BLOOMBERG SCHOOL OF PUBLIC HEALTH

This Data Use Agreement (“Agreement”) is made by and between the Maryland Health Care Commission (“MHCC” or “the Commission”), located at 4160 Patterson Avenue, Baltimore, Maryland 21215, and Center for Population Health IT, Johns Hopkins Bloomberg School of Public Health (“Data Recipient” or “JHU”), located at 624 N Broadway, Room 606 (each a “Party” and, collectively, the “Parties”), to govern the release, use, privacy and security of information from the Maryland Medical Care Data Base (“MCDB”) 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, MCDB);

**WHEREAS**, the Data Recipient, by written application dated March 7, 2022 submitted to MHCC, requested access to the following data sets:

MCDB commercial claims data files for calendar years 2016-2020 and Medicaid data claims files for calendar years 2016-2020 for a project entitled, “*Advancing Maryland's Statewide Suicide Data Warehouse to Improve Individual and Population-level Mortality Prediction and Prevention.*”

**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.

Attachments include the following:

- Attachment A – Covered Data;
- Attachment B – Scope of Work
- 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.

**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:

## **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 receive from CRISP data consisting of MCDB demographic file assigned CRISP EIDs as the primary key to enable linkage of the data sources. MHCC will incorporate the study ID into the MCDB file. MCDB 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, “Advancing Maryland’s Statewide Suicide Data Warehouse to Improve Individual and Population-level Mortality Prediction and Prevention” as described in Attachment B (“Scope of Work”), and other future projects to be reviewed and approved by MHCC. 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:

To address the challenges of suicide death prediction, in 2018 NIMH funded our team to develop the Maryland Suicide Data Warehouse (MSDW). The aim was to link a diverse set of data sources and use various layers of risk factors to predict suicide death on a generalizable population. We have since secured additional funding through an R01 grant from NIMH and expanded our aims to include (1) a refresh of existing data and acquiring new data from different sources and replication of descriptive findings, (2) develop and assess hypothesis-driven techniques to predict suicide death, (3) explore hypothesis-generating use cases of the MSDW, and (4) evaluate the generalizability of data sources and methods.

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

The primary approach of disseminating will be through published peer-reviewed manuscripts and conferences. Only aggregated results will be published. Information on individuals will not be publicly shared. Additional aggregate results may be shared with the funding agency (NIMH) as requested per NIH guidelines.

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 Within the Data Recipient's organization, access to the Covered Data, the Covered Data documentation, and any files derived from the Covered Data shall be limited 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 Protected Health Information (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 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 written approval document, entitled, *APPROVAL/DETERMINATION MEMO Continuing Review*, dated September 30, 2021, issued by the JHSPH Institutional Review Board (IRB) Office, stating an Approval/Determination Date of September 16, 2021, based on a determination that the Data Recipient’s study was “*Determined to be Exempt Cat: (4)*,” and an “*Approval Lapse Date of September 15, 2024.*” If this Agreement is still in effect on September 15, 2024 when Data Recipient’s IRB approval is scheduled to lapse, Data Recipient shall submit to MHCC staff written documentation that the JHSPH IRB has re-reviewed and re-approved Data Recipient’s study with a new approval lapse date that is later than the termination date of this Agreement. Failure of the Data Recipient to submit documentation of continuous IRB approval to MHCC staff term while this Agreement is in effect shall constitute cause for termination of this Agreement in accordance with the notice provisions of section 10.3 of this Agreement.

**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 data 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's Project Manager listed in section 8.2.1 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; changes or expansions to the Scope of Work, changes to permitted data users, changes to data access and security methods, and any 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 twenty-four (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. In the event Data Recipient receives a judicial or administrative order to disclose the Covered Data in the course of a judicial or administrative proceeding, Data Recipient shall, unless expressly prohibited by the order or law, notify MHCC in writing within 24 hours of receipt of such an order to provide MHCC the opportunity

to intervene in the judicial or administrative proceeding before the date that Data Recipient is required to comply with the 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 breach, as defined in Section 6.2, has occurred.

**6.2** “Breach” means the unauthorized acquisition, access, use, or disclosure of unsecured protected health information which 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 C.F.R. §164.402 and any future amendments thereto.

**6.3** Any breach of security or unauthorized disclosure of the Covered Data 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** 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 for breach of contract, 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 \$96,000 for the Covered Data, consisting of five (5) years of data for both Medicaid and Commercial files for 2016 – 2020. Data Recipient shall pay the one-time fee of \$96,000 in full to MHCC before any of the Covered Data is provided to Data Recipient.

7.2 No reimbursement will be made to either Party to the other Party for expenses related to accessing, maintaining, or upgrading their 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. PROJECT MANAGERS AND NOTICE

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

8.1.1 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

8.1.2 If to Data Recipient:

**Project Manager Name:**  
**Data Recipient Name**  
**Data Recipient Address**  
**Email:**  
**Telephone:**

## 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 for a period of two (2) years 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.**

For the JHU

For the Maryland Health Care  
Commission

Signed:

Signed:

\_\_\_\_\_  
[Insert Name]  
[Insert Title]

\_\_\_\_\_  
Ben Steffen  
Executive Director

Date Signed: \_\_\_\_\_

Date Signed: \_\_\_\_\_

## ATTACHMENT A – Covered Data

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

	2016	2017	2018	2019	2020
Pharmacy Claims Files	X	X	X	X	X
Eligibility Claims Files	X	X	X	X	X
Professional Health Claims Files	X	X	X	X	X
Institutional Claims Files	X	X	X	X	X

## ATTACHMENT B – Scope of Work

### ATTACHMENT A: SCOPE OF WORK

#### 1. Project Purpose

- a. Describe the specific research question(s) you are trying to answer or problem(s) you are trying to solve with the MCDB data requested (Please list and number the individual questions), or describe the intended product or report that will be derived from the requested data.

To address the challenges of suicide death prediction, in 2018 NIMH funded our team to develop the Maryland Suicide Data Warehouse (MSDW). The aim was to link a diverse set of data sources and use various layers of risk factors to predict suicide death on a generalizable population. We have since secured additional funding through an R01 grant from NIMH and expanded our aims to include (1) a refresh of existing data and acquiring new data from different sources and replication of descriptive findings, (2) develop and assess hypothesis-driven techniques to predict suicide death, (3) explore hypothesis-generating use cases of the MSDW, and (4) evaluate the generalizability of data sources and methods.

- b. Briefly describe the purpose(s) for which MCDB data are sought. Use quantitative indicators of public health importance where possible, for example, variation in costs of care; rates of under or over service utilization; health system performance measures, the effect of public health initiatives, health insurance, etc.

Suicide is the 10th leading cause of death in the US. Despite the loss of over 48k lives a year, suicide death is a rare event and challenging to predict. Moreover, suicide does not have individual risk factors with high positive predictive value for death that are captured in routine clinical data. Thus, studies have often struggled to integrate multiple risk factors to predict suicide death across generalizable patient populations. This has left most research into predicting suicide deaths dependent on models developed for specific subpopulations such as veterans, arm soldiers, and psychiatric patients. The goal of this study is to leverage data from multiple sources including that from the Maryland Health Care Commission, hospital discharges, and office of medical examiner (OCME) data. Linking these data sources will allow for novel secondary data analyses which will enhance our understanding of risk of suicide death and allow outreach and interventions to be deployed in a timely manner. The predictive models could provide insight into the timing and nature of predictors as well as gaps in care.

- c. Explain in detail how the planned project that will use MCDB data is in the public interest and give specific examples of how the project will serve the public interest.

We have previously shown that linking data is underutilized in youth suicide prevention. Data from payer claims database, mortality data, surveillance data, and electronic health records could be linked to data from suicide prevention efforts to help identify which interventions are most effective in preventing suicidal behaviors, and who benefits from specific interventions and what under what conditions. Our predictive models of suicide death will be in the public domain and can be adopted by various health systems and insurers.

#### 2. Project Methodology

- a. Provide a written description of the project methodology, state the project objectives, the protocol, software and/or identify relevant study questions and analysis method to allow MHCC to understand how the MCDB Data will be used to meet project objectives or address research questions.

**Data Sources & Linkage:** This is a retrospective study using limited data from various data sources including MHCC MCDB data. We are requesting MCDB (a.k.a., APCD) files at an individual level between 2012 and 2020 for Maryland residents. We understand that 2019 and 2020 data will become available later. CRISP (Maryland's HIE) will receive the MCDB data (if not already available to them), assign an encrypted research ID (EID), and share a limited dataset with the research team at Johns Hopkins. The limited data will include age in years, dates of service, and census block group information. The research team will not receive any protected health information (PHI) except the limited data. The EID is used by the research team to link MCDB data to OCME (office of medical examiner) records. CRISP has also anonymized and tagged OCME data with EID before sharing it with the research team. The EID will be unique to this study and not linked to other data sources outside of this study. Any PHI data provided to CRISP, including MHCC ID, will be used only by CRISP to identify individuals and assign the appropriate study EID as needed.

**Study Aims & MCDB:** This study aims to better identify patients who may commit suicide. We will develop a series of suicide prediction models to achieve this. MCDB data will provide the research team with clinical data (e.g., diagnostic codes, medications, encounters) that have shown to be predictive of suicide death. The limited data elements (i.e., age, dates of encounter, census block group info) are also vital to the construction of the predictive modeling process (e.g., better construct the trajectory of a temporal predictive model, better understand the neighborhood effect on suicide outcome).

**Methods:** We will compare individuals who have died by suicide to those who have died by other means as specified in the OCME data. We are also requesting the living patients from MHCC to build a complete control population as recommended by the National Institute of Mental Health (NIMH). Having this control population will allow us to develop a more generalizable prediction model. Once the data is linked, we will develop the predictive analytics using statistical approaches to identify suicide deaths. Using the linked data, we will construct a retrospective case-control study exploring suicide as recorded by the medical examiner and other causes of death. We will first use logistic regression to develop a basic model for suicide risk and compare to other models. We will build the model by using stepwise and LASSO Penalization selection including possible pairwise interactions between variables. Cross-validation will be conducted to fine tune the parameters and avoid over-fitting, especially among the living population. Other more sophisticated models will be used once the data is refreshed and models are explored. Analysis will be stratified by race, sex, insurance type and other attributes as needed.

### **ATTACHMENT C – Additional Data Sources**

- ▶ OCME data using CRISP hashed/encrypted ID.
- ▶ The Health Services Cost Review Commission (HSCRC)
- ▶ Johns Hopkins Health System
- ▶ Anne Arundel Medical Center
- ▶ Peninsula Regional Medical Center
- ▶ Veteran's Health Administration of Maryland, and CRISP Insight

DRAFT

**ATTACHMENT D – Data Users Log**

**DATE OF LAST UPDATE:** \_\_\_\_\_

Data Recipient shall keep a log of the identity of each individual who is authorized to access the data provided under this Agreement. This Attachment 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 shall provide written updates of this log to MHCC before authorizing any new individual to access the Covered Data.

By signing my name below as a Data User, I certify that I have reviewed this *DATA USE AGREEMENT BETWEEN THE MARYLAND HEALTH CARE COMMISSION AND*

**Data Recipient**

**Name** \_\_\_\_\_.

I understand the confidential nature of the Covered Data and I agree to abide by the required safeguards to protect the security of the data. I understand that the Covered Data can only be used for “Permitted Uses” identified in section 2 of this Agreement and can only be shared with individuals listed and approved in this Data Users Log.

**Data Recipient Personnel with Access to MCDB Data:**

<b>Name of Data User</b>	<b>Title</b>	<b>Unit</b>	<b>Signature</b>	<b>Date</b>






**ATTACHMENT E – Data Management Plans and Data Storage Locations**  
***(JHU's DMP/Data Storage Location needs to be inserted here before DUA is signed)***

**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** [REDACTED]

have been destroyed.

<b>Project Title</b>	[REDACTED]
<b>MHCC DUA Number</b>	[REDACTED]
<b>Principal Investigator Name</b>	[REDACTED]
Title	[REDACTED]
Organization	[REDACTED]
Address	[REDACTED]
Tel Number	[REDACTED]
Fax Number:	[REDACTED]
E-mail Address	[REDACTED]
<b>Data Custodian Name</b>	[REDACTED]
Title	[REDACTED]
Organization	[REDACTED]
Address	[REDACTED]
Tel Number	[REDACTED]
Fax Number	[REDACTED]
E-mail Address	[REDACTED]

**Date the Data was Destroyed:**

**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:**

**Principal Investigator**

Organization:

Signature

Printed Name

Title

**Data Custodian**

Organization:

Signature

Printed Name

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