



Application for Maryland Medical Care Data Base

TRACKING TABLE (For MHCC Use Only)

MHCC Data Request Number	
Application Received	
Application Approved	
Data Obtained	

INSTRUCTIONS

This form is required for all Applicants requesting MCDB data. Applicants must also complete all the attachments. The completed Application and the Data Management Plan will be used by MHCC to determine whether the request meets the criteria for data release, pursuant to COMAR 10.26.06. Incomplete Applications will be returned to the Applicant, and the request will be delayed. All Applications require a nonrefundable application fee, payable at the time of submission.

Where to submit documents:

- Completed application packages should be scanned and emailed to: mhcc.datarelease@maryland.gov
- A hard copy Application is acceptable and should be sent, with the application fee, to:
Maryland Health Care Commission
4160 Patterson Avenue,
Baltimore, MD 21215,
ATTN: MHCC Data Release
- Please enclose a cover note page that includes the project title, requesting organization's name, and applicant's name.
- If an invoice is needed, please send a request to: mhcc.datarelease@maryland.gov

Note to Applicants:

- Review [data availability and fees](#)
- All Application attachments will be incorporated into the Approved Data Use Agreement (DUA)

Questions? Email mhcc.datarelease@maryland.gov

TABLE OF CONTENTS

INSTRUCTIONS	1
PROJECT INFORMATION	3
ATTACHMENT A: SCOPE OF WORK	4
ATTACHMENT C: ADDITIONAL DATA SOURCES AND LINKAGE	8
ATTACHMENT D: DATA MANAGEMENT PLAN	10
ATTACHMENT E: USE OF CONTRACTORS AND/OR CONSULTANTS (External Entities)	15
ATTACHMENT F: APPLICANT QUALIFICATIONS	16
ATTACHMENT G: OBLIGATIONS AND ATTESTATION	17

PROJECT INFORMATION

Project Title			
Scheduled Project Start Date		Scheduled Project End Date	
MHCC Staff Approved Pre-Application Number			
Project Overview: <i>Provide an abstract or brief summary (150 words) of the specific purpose and objectives of the Project.</i>			

Applicant <i>(principal investigator, project manager, individual responsible for the research team using the data)</i>			
Name			
Title			
E-Mail Address			
Telephone Number			
Organization Name			
Mailing Address			
City/Town		State	
		Zip Code	

Requesting Organization <i>(Agency, Academic Institution, Research Organization, Company, etc.)</i>			
Organization Name			
Website			
E-Mail Address			
Telephone Number			
Mailing Address			
City/Town		State	
		Zip Code	

Data Custodian <i>(person responsible for receiving, organizing, storing, and archiving data)</i>			
Name			
Title			
E-Mail Address			
Telephone Number			
Organization/Company <i>(if different from Requesting Organization)</i>			
Mailing Address			
City/Town		State	
		Zip Code	
Relationship to Requesting Organization <i>(e.g., Contractor)</i>			

Project Contact <i>(person responsible for all communications with MHCC)</i>			
Name			
Title			
E-Mail Address			
Telephone Number			
Organization Name			
Mailing Address			
City/Town		State	
		Zip Code	

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.

- 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.

- 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 serves the public interest.

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.

- b. Do you have approval for your project from an Institutional Review Board (IRB)? All Applicant must obtain review by an Institutional Review Board that has been or will be recognized by the MHCC.
- Yes (attach a copy of the approval to this application)
 - No

Enter date submitted to IRB Name of the IRB

3. Publication and Dissemination

Briefly (1-3 sentences) explain any "Yes" answer.

- a. Do you anticipate that the results of your analysis will be published or made publicly available?
- Yes
 - No

- i. If yes, how do you intend to disseminate the results of the study (e.g., publication in a professional journal, poster presentation, newsletter, web page, seminar, conference, statistical tabulation, etc.)?

- ii. All public displays of MCDB data, regardless of the medium must comply with MCDB's cell size suppression policy, as set forth in the Data Use Agreement. Please explain how you will ensure that any public display will not disclose a cell size (suppression) that is less than 11, and percentages or other mathematical formulas that result in the display of a cell size (suppression) that is less than 11.

- iii. Identify the lowest geographical level of analysis of data you will to present for publication or presentation (e.g., state level, city/town level, zip code level, etc.). Will maps be presented? What methods will be used to ensure that individuals cannot be identified?

- b. If you answer "yes" to any of the following questions, describe the types of products, software, services, or tools and the corresponding fees will for such products, software, services, or tools.

- i. Will the MCDB data be used for consulting purposes? Yes No

- ii. Will report(s), website(s) or a statistical tabulation(s) using MCDB data be shared or sold? Yes No

iii. Will a software product using MCDB data be shared or sold? Yes No

iv. Will MCDB data be used as input to develop a product (i.e., severity index tool, a risk adjustment tool, a reference tool, etc.)? Yes No

v. Will MCDB data be sold or shared in any format not noted above? Yes No

If yes, in what format and who are the purchaser of the data?

vi. Will the project result in disclosing MCDB data, or any data derived or extracted from such data, in any paper, report, website, a statistical tabulation, seminar, or another setting that is not disseminated to the public? Yes No

vii. Will the results from the project be used for price transparency? Yes No

viii. Will health care providers be individually identified? Yes No. Please describe your protocol for informing health care providers.

ATTACHMENT B: MCDB DATASET REQUESTED

MHCC collects privately insured data (claims and membership), known as the Medical Care Data Base (MCDB), on a quarterly basis from life and health insurance carriers, health maintenance organizations (HMOs), third party administrators (TPAs), and pharmacy benefits managers (PBMs) that are licensed to do business in Maryland. The MCDB data that is available for release contains eligibility and professional, institutional, and pharmacy claims. Starting in 2015, the Medical Care Data Base (MCDB) excludes private plan data for self-insured ERISA due to the *Gobeille v. Liberty Mutual* Supreme Court ruling.

The data which is refreshed and updated annually contains only privately fully-insured and self-insured non-ERISA health insurance plans for Maryland and non-Maryland residents. The MCDB comprises of about 90-95% of the privately fully insured market and just about 25% - 30% of the self-insured market (post-Gobeille, primarily non-ERISA). To determine the years for which data are available check on the [MHCC website](#). That site also contains information about the most current MCDB Release Version and a full list of elements in the release including the release record layouts, data dictionaries, and supporting documentation.

1. Which MCDB files are you requesting? Provide a brief justification (1-3 sentences) for each one.

Dataset	Year(s)
<input type="checkbox"/> Institutional Claims	
<input type="checkbox"/> Professional Claims	
<input type="checkbox"/> Pharmacy Claims	
<input type="checkbox"/> Member Eligibility	

ATTACHMENT C: ADDITIONAL DATA SOURCES AND LINKAGE

1. Medicaid Data

Applications for access to Medicaid Managed Care data for studies comparing the privately insured to Medicaid Managed Care patients can be submitted, but require a separate approval from the Maryland Medicaid Administration. The fields available on the Medicaid MCO data sets have been aligned with MCDB fields to the extent possible.

- a. Indicate whether you are seeking Medicaid data: Yes No
- b. Do you intend to merge or link MCBDB data with Medicaid data? Yes No
If yes, provide brief justification.

- c. Federal law (42 USC 1396a (a) 7) restricts the use of individually identifiable data of Medicaid recipients to uses that are directly connected to the administration of the Medicaid program. If you are requesting Maryland Medicaid Data, please describe, in the space below, why your use of the Data meets this requirement.

2. Other Linkages

Data linkage involves combining MCDB data with other data to create a more extensive database for analysis.

1. Do you intend to merge or link MCBDB Data with other data? Yes No

If **Yes**:

- a. What are the files to be linked?

- b. Why is this linkage needed?

- c. Which MCDB data elements will be linked to the data elements in the external file?

- d. What methodology or algorithm will be used to create this match? If you intend to create a unique algorithm, please describe how it will link each dataset.

e. What variables from each of the source files will be included in the final linked analytic file?

2. Explain why the linkages are needed.

3. Describe the specific steps the Organization will take to prevent the identification of individuals in the linked files.

ATTACHMENT D: DATA MANAGEMENT PLAN

Certification

The undersigned certifies and agrees as follows:

- The data will be used only for approved purposes of analysis and presentation.
- The Organization will comply with all administrative, technical, and procedural policies and physical safeguards established to protect the confidentiality of the data and to prevent unauthorized access to the data.
- The data will be encrypted at rest and on motion on storage media (backup tapes, local hard drives, network storage, et al.) with at least an AES-256 standard or stronger.
- The Organization understands and agrees that any intentional breach of confidentiality will result in termination of the Data Use Agreement.
- Anti-virus software or service is active on any server or endpoint containing the MCDB data.
- Staff with access to PHI or other sensitive data have received all relevant training

The Organization has policies and procedures in place to address:

- The sharing, transmission, and distribution of PHI
- The physical possession and storage of PHI
- The destruction of PHI upon completion of data use
- Confidentiality agreements with each individuals, including contractors, who will access PHI
- Agreements governing the use and disclosure of PHI with all non-employees who will access PHI

Confirm you certify and agree to the above statement

1. Responsible Individuals

a. Provide the name(s) of custodian responsible for receiving, organizing, storing, or archiving data.

Name					
Title					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town		State		Zip Code	

b. Provide the name of the person who will notify MHCC of any breach of the MCDB data, Data Use Agreement or the Data Management Plan

Name					
Title					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town		State		Zip Code	

c. Provide the name of the person responsible for ensuring proper data destruction upon the termination of the Data Use Agreement, and submission of the Certification of Data Destruction.

Name					
Title					
E-Mail Address					
Telephone Number					

Organization Name					
Mailing Address					
City/Town		State		Zip Code	

- d. Provide the name of the person who will notify MHCC of any project staffing changes, maintain the roster of staff who have formal, documented permission to access specific files for specific purposes, and ensure that all individuals with access to the data comply with the Data Use Agreement.

Name					
Title					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town		State		Zip Code	

2. Physical Possession and Storage of Data Files

1. List how the data will be stored.
 - Cloud
 - Physical location(s)
 - Both
2. Provide the delivery address for the data, including the location where the data will be stored.

i. Delivery Address

Address					
City/Town					
State		Zip Code			

ii. Storage Address

Address					
City/Town					
State		Zip Code			

3. Provide the name and address of the Cloud Service Provider

Address					
City/Town					
State		Zip Code			

4. Describe the name and data security assessment level of each physical location and the Cloud Service Provider where the data will be stored. Provide evidence that the proposed computing environment meets or exceeds NIST 800-53v4 security standards. Identify all certifications held by entities that will store or hold data.

- a) SOC 2 Type Audit
- b) HITRUST Certification
- c) ISO 27001 Audit Certification
- d) Independent external HIPAA standards Assessment
- e) SSAE 16 Overview, and/or
- f) FedRAMP Certification

--

5. Has each individual who will access the data agreed to the Request Organization's privacy and security rules when using MCDB data files? Yes No
6. Within the last 12 months, has each individual who will access MCDB data received training on the proper handling of protected health information and/or personal data? Yes No. If no provide a brief description of the circumstances and detail the training that each such person will receive and by what date.

7. Explain the infrastructure (facilities, hardware, software, etc.) that will secure the MCDB data files.

8. Briefly describe the policies and procedures regarding the physical possession and storage of MCDB data files.

9. Briefly describe the system or the process to track the status and roles of the individuals with access to the MCDB data files.

10. Briefly describe physical and technical safeguards that will be used to protect MCDB data files.

11. Briefly describe how the data will be backed up and how back up files will be managed.

3. Data Sharing, Electronic Transmission, and Distribution

1. Briefly describe the Requesting Organization's policies and procedures regarding the sharing, transmission, and distribution of sensitive data files (including Data Sharing Agreements).

2. Describe the Requesting Organization's policies and procedures be applicable to the physical removal, transport, and transmission of MCDB data files.

3. By checking the boxes next to the following statements, you are confirming that the following requirements will be met.
- Access to the data will be restricted to authorized users by requiring computer log-on with unique user accounts and passwords.

For data stored on a network drive and not on your computer hard drive:

- Access will be restricted by limiting folder access to approved study staff only.
- Any data included in the network backup will be encrypted.

For data stored on the local hard drive of a computer:

- When not in use, the computer will be locked in a physically secured office, drawer, cabinet or other container to which access is restricted to authorized study personnel.
- When not in use, data will be encrypted with a key length of at least 256 bits.

4. Describe the Requesting Organization's technical safeguards for data access place:

Password protocols:
Log-on/log-off protocols
Session time out protocols
Encryption for data in motion and data at rest
Antivirus and anti-malware products

5. If applicable, describe the Requesting Organization's physical safeguards for data access and check all security features listed below that are present in the room containing MCDB data files:
- Recorded video
 - Access log of all individuals entering the room
 - Secure server rack
 - Access control limiting access only to authorized individuals
6. If applicable, identify the data transmission method(s) you plan to use.
- VPN
 - Secure FTP

Encrypted email delivery system

Other, please specify and identify why this meets minimum data security requirements below:

7. Describe the Requesting Organization's policies and procedures to protect sensitive data files when individual staff members of project teams (including additional collaborating organizations) terminate their participation on a project. (May include staff exit interviews and immediate access termination).

4. Completion of Research Tasks And Data Destruction

Applicant must agree that the MCDB data, all copies and backups must be destroyed immediately after the period of time necessary to fulfill the requirements of the data request in accordance with the terms and conditions of the Data Use Agreement. All data destruction must follow and conform to [NIST Special Publications 800-88, Guidelines for Media Sanitization](#).

1. Describe the Requesting Organization's process to complete the Certificate of Data Destruction form and the Requesting Organization's policies and procedures to destroy data files upon completion of the project.

2. If a copy of the data is needed to be maintained for a longer period, please provide the reason a longer time period is necessary.

ATTACHMENT E: USE OF CONTRACTORS AND/OR CONSULTANTS (External Entities)

Provide the following information for all consultant and contractors who will have access to the MCDB data. The Requesting Organization must have a written agreement with the contractor/consultant to ensure the use of MCDB data to the approved project(s) of this application as well as the privacy and security standards set forth in the Data Use Agreement. MCDB data may not be shared with any third party without prior written consent from MHCC, or an amendment to this Application.

Entity	<input type="checkbox"/> Contractor			<input type="checkbox"/> Subcontractor			<input type="checkbox"/> Consultant		
Organization Name									
Title									
Website									
Contact Person									
E-Mail Address									
Telephone Number									
Mailing Address									
City/Town				State			Zip Code		
Term of Contract									

1. Describe the tasks and products assigned to this entity for this project.

2. Describe the qualifications of this entity to perform and complete the tasks.

3. Describe the Requesting Organization's oversight and monitoring of the activities and actions of this entity for this project, including how you will ensure the privacy and security of the MCDB data to which the consultant or contractor has access.

4. Will this entity have access to or store the MCDB data at a location other than the data custodian location, off-site server and/or database? Yes No.

If yes, a separate Data Management Plan **must** be completed by this contractor/consultant.

[INSERT A NEW SECTION FOR ADDITIONAL CONTRACTOR/CONSULTANT ENTITIES NEEDED]

ATTACHMENT F: APPLICANT QUALIFICATIONS

1. Describe previous experience using claims data. This question should be answered by the primary investigator/project manager and should encompass the experience of the entire project team who will be using the data.

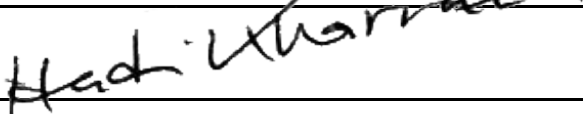
2. Resumes/CVs: When submitting your Application package, include résumés or curricula vitae of the principal investigator/project manager and any project team with relevant experience

ATTACHMENT G: OBLIGATIONS AND ATTESTATION

ATTESTATION OF APPLICANT

I, _____, Applicant, solemnly affirm under penalties of perjury that the information contained in the Application its attachments, and this Attestation, is true and correct to the best of my knowledge, information and belief and that the requested MCDB data is the minimum necessary to accomplish the Project. I accept my obligation to comply with all requirements in this Application and attachments, including:

- (1) Compliance with all data privacy and security obligations;
- (2) Execution of a Data Use Agreement approved by MHCC-staff prior to receipt of the requested data;
- (3) Responsibility for assuring that the data has been destroyed at the conclusion of the project in accordance with the terms and conditions of the Data Use Agreement;
- (4) Responsibility for assuring that specified MHCC staff is notified within 30 days when any person who has access to the MCDB data is removed from or added to the MHCC-approved Project;
- (5) Responsibility for assuring that each required report is sent to the MHCC staff within the time period specified in the Data Use Agreement; and
- (6) Continuing compliance with the Data Management Plan.

Applicant's signature:	
Printed Name:	
Title:	
Date:	

ATTESTATION OF REQUESTING ORGANIZATION

I, _____, _____ of _____, the Requesting Organization in this Application, have been duly authorized by the Requesting Organization to execute this attestation on its behalf. I solemnly affirm under penalties of perjury that the information contained in the Application, its attachments, and this Attestation, is true and correct to the best of my knowledge, information and belief.

Signature of authorized representative of the Requesting Organization:	
Printed Name:	
Title:	
Date:	