Colorado All Payer Claims Database
Data Release Application

Thank you for your interest in obtaining data from the CO APCD. As you fill out this application, please let us know if you have any questions or concerns by reaching out to ColoradoAPCD@civhc.org. We are here to help!

Also, please be aware that if you are requesting Protected Health Information (PHI), your request requires a recommendation for approval by the Data Release Review Committee (DRRC). Data elements that are considered PHI under HIPAA are indicated below. If PHI is requested, a CIVHC Account Executive will help you successfully complete an application and navigate the DRRC process.

Please use this application to submit information regarding your request for data from the Colorado All Payer Claims Database (CO APCD). This information will help the Center for Improving Value in Health Care (CIVHC), the Administrator of the CO APCD, answer any questions you have regarding your data request and assist us in helping you complete the data application form.

Note: Please reference the CO APCD Data Elements Request Form found at http://www.civhc.org/get-data/data-release/ when completing this form.

Introduction: Section 10 CCR 2505-5-1.200.5 describes how the CO APCD Administrator addresses Requests for Data and Reports:

1.200.5.A. A state agency or private entity engaged in efforts to improve health care or public health outcomes for Colorado residents may request a specialized report from the CO APCD by submitting to the administrator a written request detailing the purpose of the project, the methodology, the qualifications of the research entity, and by executing a Data Use Agreement (DUA), to comply with the requirements of HIPAA.

1.200.5. B. A data release review committee shall review the request and advise the administrator on whether release of the data is consistent with the statutory purpose of the CO APCD, will contribute to efforts to improve health care for Colorado residents, and complies with the requirements of HIPAA. The administrator shall include a representative of a physician organization, hospital organization, non-physician provider organization and a payer organization on the data release review committee.

This Data Release Application serves as the written request for information noted in section 1.200.5.A.

PART ONE

Project Information	
Project Title:	20.59 Continuity of Medicaid Under the Affordable Care Act
Date:	2/7/2020
Organization Requesting Data:	Boston University, Department of Health Law, Policy, and Management
Contact Person:	Sarah H Gordon
Title:	Assistant Professor
E-mail:	gordonsh@bu.edu
Phone Number:	617-358-1864
Person Responsible for the Project (if different than above):	
Title:	
E-mail:	
Phone Number:	

Project Purpose:

Project questions to be discussed with client representative:

- Please describe your project and project goals/objectives.

The research project entitled "Continuity of Medicaid Coverage under the Affordable Care Act" seeks to evaluate the effect of policies in the 2010 Affordable Care Act (ACA) on stability of coverage among Medicaid beneficiaries in Colorado. While analyses suggest ACA policies have been effective in reducing the number of uninsured CO residents, existing assessments of the uninsured capture only a snapshot in time, when health insurance coverage is dynamic.

Health insurance "churning" is defined as unnecessary cycling off and on coverage, and is particularly important for pregnant women who experience frequent coverage changes before and after delivery. Nationally, 62% of women experience at least one change in insurance status during the prenatal period and 47% of women experience a coverage lapse within six months postpartum. Such periods of uninsurance have detrimental effects on maternal and child health outcomes, and potentially lead to preventable hospitalizations and emergency department visits. Characterizing pregnant women's enrollment patterns across different insurance types and quantifying their health effects before and after Colorado expanded Medicaid will provide critical insights into risk factors for poor postpartum maternal health and identify factors that contribute to racial/ethnic health disparities in the state.

- What specific research question(s) are you trying to answer or problem(s) are you trying to solve with this data request? (Please list and number the individual questions.)

- We seek to characterize changes in insurance coverage among pregnant Medicaid beneficiaries over time and between sources of coverage.

-We seek to evaluate the impact of perinatal insurance disruptions on the presence of severe maternal morbidity at the time of delivery, inpatient and emergency department use in the postpartum period, and access to postpartum mental health services.

-We will investigate whether health insurance changes contribute to maternal health disparities between Hispanic/Latina mothers and white mothers.

- How will this project benefit Colorado or Colorado residents? (this is a statutory requirement for all non-public releases of CO APCD data)

The proposed project benefits Colorado residents because it is specifically focused on improving the quality of care delivered to low-income pregnant women and mothers in the state of Colorado. This proposal addresses a national crisis in maternal health. In Colorado, the maternal mortality rate doubled between 2008-2013, demonstrating a disproportionate burden of mortality among low-income residents of color.

Our work could provide the Colorado Department of Health Care Policy & Financing with an assessment of how stable Medicaid coverage is for pregnant women in Colorado and the downstream consequences of gaps or changes in perinatal coverage on clinical quality and population health for pregnant women and new mothers. This information can directly inform policy strategies to improve maternal health among pregnant women and new mothers with discontinuous Medicaid enrollment.

- Please answer all applicable questions below (Note that your project must meet one or more of the Triple Aim criteria below to generate a benefit for Colorado):
    - If applicable, how will your project support lowering health care costs?

This proposal supports lowering health care costs because it will help identify inefficiencies in the delivery of maternity services throughout the perinatal and postpartum (~1 year after birth) periods. One of the comparisons we will conduct will compare healthcare costs among women who are covered via Medicaid versus other coverage after delivery. We will compare both out-of-pocket and total costs across insurer type to identify the most cost-effective way to provide continuous access to services during the transition from postpartum to well-woman care. In addition, this proposal seeks to identify downstream system-level cost consequences associated with insurance changes, such as higher outpatient and emergency department use due to a lack of continuity during the high-risk postpartum period.

    - If applicable, how will you project help improve the health of Coloradans?

This proposal seeks to alleviate the burden of maternal morbidity and mortality in Colorado by investigating policy determinants of maternal health disparities between white mothers and Hispanic mothers and examining how interruptions in coverage and continuity of care may increase risk of postpartum maternal morbidity.

    - If applicable, how will your project improve the quality of care or patient experience?

Coverage stability is key to the delivery of quality care because gaps or changes in coverage status can result in beneficiaries delaying or forgoing care, facing high medical bills, or otherwise slipping through the cracks of the delivery system. NCQA includes postpartum visits, postpartum mental health screenings, and

postpartum contraception access as important indicators of quality for maternity services. We will examine the probability of women receiving these quality indicators depending on whether they change insurance postpartum. In addition, we will examine continuity of care – an important driver of positive patient experience.

- Do you need a claims data set or would you like a custom report generated by CIVHC that addresses the specific questions/problems your project seeks to address? Claims data set

- Do you need Protected Health Information (PHI)? Yes
    - Do you need patient-specific dates (e.g., dates of service or DOB) or 5 digit zip code. If so, this is a request for a Limited Data Set.

- Do you need direct patient identifiers such as name, address, orcity? If so, this is a request for an Identifiable Data Set (requires IRB approval).
- If you do not require any PHI, please only complete PART ONE of the application.

Please note: your CIVHC representative will work with you to complete **Addendum I – Analyst Supplement** to address data warehouse specific questions.

If you are requesting a Custom Report with analytics to be provided by CIVHC; please stop here and submit the information above to your CIVHC representative.

PART TWO

1. Type of CO APCD Analytic Data Set Requested

Please select the type of data set that you are requesting by checking one of the boxes below (**select only ONE option**). Details on each type of CO APCD data set can be found in *The CO APCD Companion Instruction Guide* (available from your CIVHC representative):

Types of Analytic Data Sets (Please select ONE below)

For users interested in a wide range of data to analyze on their own.

☐ De-Identified Data Set
☒ Limited Data Set*
☐ Identified Data Set *

*These types of data requests include Protected Health Information (PHI). Under HIPAA, PHI may only be released in limited circumstances for public health, health care operations, and research purposes under the terms of a HIPAA compliant data use agreement (DUA).

2. Requested Data Elements

The CO APCD is committed to protecting the privacy and security of Colorado's health care claims data. The CO APCD will limit the use of the data to purposes permitted under applicable laws, including APCD Statute/Rule and HIPAA/HITECH, to information reasonably necessary to accomplish the project purpose as described in this Application.

Data Element Selection and Justification

If you have not already done so, please use the Data Element Dictionary (DED) to identify the specific data elements that are required for this project. In keeping with the minimum necessary standard established under HIPAA, CO APCD policy is to release only those data elements that are required to complete your project.

Type of Data	Justification for Elements on the DED
Names	N/A
Street Address	N/A
City	N/A

Zip Code	Five-digit zip codes are necessary to control for area-level factors at a sufficiently granular level of measurement.
Health Plan Beneficiary Numbers	N/A
Dates (including Day and Month detail.) Specify which date fields are needed and why.	In order to assess the utilization of health services and enrollment in health coverage, precise dates of service and enrollment are required.
Payer Name	Because our analysis measures the impacts of gaps and transitions in health insurance coverage, we require information on who the health insurance payer is in order to track these changes accurately.
Provider Identifying Information	Our analysis seeks to assess whether Medicaid beneficiaries who have a change or gap in health insurance experience continuity of care afterwards, defined as seeing the same providers. To measure this outcome, we require unique provider identifiers (but not necessarily any personal or identifiable information) to measure consistency of providers.
Vital Statistics Birth Records	Race/ethnicity information from the birth certificate is required as demographic information is limited in the claims.
Income for female Medicaid enrollees, ages 19-50	Income is associated with many health outcomes and measures of health utilization. Individual-level income is required for Medicaid enrollees in order to control for this important driver of patient-level differences.

A. Counts, Totals and other Summary Statistics

The CO APCD seeks to provide aggregated summary data whenever possible. Applicants are encouraged to request counts, totals, rates and other summary values whenever such information can reasonably accomplish the purpose of the project (add rows to the table below if necessary). The CO APCD supports the federal CMS minimum cell size suppression policy that requires any cell in any report or data table, printed or electronic, with less than eleven records or observations to be replaced by "Less than eleven" or similar text. You must also apply complementary cell suppression techniques to ensure that cells with fewer than eleven records cannot be identified by manipulating data in adjacent rows and columns.

Field Number and Name	Requested Count or Sum
	[add rows as needed]

B. Linkages to Other Data Sets

The CO APCD seeks to ensure that data cannot be re-identified if it is linked to or combined with information obtained from other sources. If this project requires claims line level detail or includes linkages to other databases, or if CO APCD data will be combined with other information, provide a justification for each proposed linkage. Be sure to describe how this will contribute to achieving the project purpose, including whether the project can be completed without this linkage, and the steps you will take to prevent the identification of individual patients:

Will you link the CO APCD data to another data source?

☐ No.
☒ Yes. If yes, please answer the following questions.

- Which CO APCD identifying data elements will be used to perform the linkage?

The APCD will be linked with vital statistics birth records using identifiable data and income data from Health First Colorado. Only the final deidentified linked data will be provided to the research team.

- Once the linkage is made, what non-CO APCD data elements will appear in the new linked file?

Data elements from Colorado birth records and individual-level income for female Medicaid enrollees 19-50.

- Have all necessary approvals been obtained to receive and link with the other data files (e.g., IRB or Privacy Board approval)? Yes

C. Distribution of the Report or Product:

Prior Review by the CO APCD Administrator

If you are producing a report for publication in any medium (print, electronic, lecture, slides, etc.) the CO APCD Administrator must review the report prior to public release. The CO APCD Administrator will review the report for compliance with CMS cell suppression rules; risk of inferential identification; and consistency with the purpose and methodology described in this Application.

- Please describe your audience and how to you will make your project publicly available?

The results of this research will only be public insofar as results in aggregated and de-identified forms will be disseminated for publication in peer-reviewed academic journals and presentedat national conferences. The proposed audience for this the published manuscripts that utilize these data includes the health policy, health economics, and health services research communities, health policy analysts, policymakers, state and federal Medicaid officials, health insurers, and providers.

- If the report is not to be made publicly available, then briefly describe how the information derived from this data will be used and by whom:

Other Organizations: Do you intend to engage third parties who will have access to the data requested as part of this project? If so, list the organizations below, describe their role(s); and explain why they will be granted access to the requested data.

Organization/Company Name:	
Contact Person:	
Title:	
Address:	
Telephone Number:	
E-mail Address:	
Role or responsibility in this project	*[add rows as needed]*

Project Schedule:

Proposed Project Start Date:	March 1, 2020
Project End Date:	March 1, 2025
Proposed Publication or Release Date:	Fall 2020-Spring 2021
End of Date Retention Period:	Fall 2025

D. Frequency

Data in the CO APCD is refreshed monthly and data products can be provided on a one time basis or under a subscription model (e.g., quarterly, bi-annually or annually). Please select frequency below.

☐ One Time

OR

Subscription (Please select subscription model below)

☐ Quarterly
☐ Bi-annually
☒ Annually

E. Project Reporting

CIVHC highlights projects and data analysis on the public website: www.civhc.org/change-agents. This display of CO APCD projects provides future data requesters with ideas of how they can structure their analysis, and allows CIVHC's stakeholders to see how CO APCD data recipients are working to accomplish the Triple Aim for Colorado. Data recipients have the option of choosing whether to be identified or to not beidentified.

☒ Yes, it is okay for CIVHC to identify my organization
☐ No, I do NOT wish for CIVHC to identify my organization

PART THREE

DATA MANAGEMENT PLAN (Not applicable for Custom Report Requests)

I. Organizational Capacity

As an Attachment, please provide copies of the Data Privacy and Security Policies and Procedures for the Requesting Organization as well as those of any third parties that will have access to the requested CO APCD data.

- Has the Requesting Organization or any member of the project team ever been involved with a project that experienced a data security incident? If so, describe the incident, the response procedures that were followed and any subsequent changes in procedures, processes or protocols to mitigate the risk of further events.

No security incidents have occurred involving the requesting research team or among members of the project team, nor any claims data-related security incidents. Broader university-wide incidents have been reported and resolved with sanctions, training, and reporting as required by state and federal law.

To the extent that the Data Privacy and Security Policies and Procedures, provided as an Attachment, do not already do so, please answer or attach answers for the following:

- **Physical Possession and Storage of CO APCD Data Files:**
  - Describe how you will maintain an inventory of CO APCD data files and manage physical access to them for the duration of the project:

All incoming sensitive data is received and inventoried by Boston University School of Public Health Biostatistics and Epidemiology Data Analytics Center (BEDAC). ~~Medical Campus Information Technology Services.~~ A catalog is maintained as a spreadsheet by the researcher. ~~Physical media are retained in a locked cage within a locked card-access server room.~~ Online copies are maintained on a secure system, described in the Secure Data Center Policy (available from: http://www.bu.edu/tech/about/policies/secure-data-center-access/). ~~disks housed within the same cage, dedicated to BUMC computing infrastructure for research. Access to this space is strictly monitored and requires key card entry and a pin code in an area with 24-hour video surveillance. Only IT computing staff are allowed access. All authentication attempts to operating systems and applications, both successful and failed, must be locally logged. These audit logs should be forwarded to an enterprise log repository where possible.~~

~~o~~ Describe your personnel/staffing safeguards, including:

- Confidentiality agreements in place with individuals identified as being assigned to this study. Include, for example, agreements between the Principal Investigator or Data Custodian and others, including research team members, and information technology and administrative staff:

All users of BUMC IT computing infrastructure are required to undergo confidentiality training and are subject to Boston University's Data Protection Requirements. Confidentiality agreements will be established between the Principal Investigator, Data Custodian, and data analysts.

- Staff training programs you have in place to ensure data protections and stewardship responsibilities are communicated to the research team:

All BUMC researchers are required to maintain the CITI certification for Responsible Conduct in Research Training online modules and a specific BUMC-specific course on HIPAA and research data security. This

Formatted: Body Text, Indent: Left: 0.08", Right: 0.13", Space Before: 0.05 pt, Line spacing: single, No bullets or numbering, Tab stops: Not at 1.58" + 1.58"

course covers privacy and confidentiality, data stewardship, data protection, and protection of human subjects. All BUMC IT personnel take HIPAA training for IT annually.

- Procedures to track the active status and roles of each member of the research team throughout the project and a process for notifying the CO APCD of any changes to the team:

In order to gain access to any data or computing resources, including any data held under this DUA, a user must be granted a computer account and be joined to the proper security group. The Principal Investigator is required to inform Boston University Medical Campus Information Technology Services and the CO APCD administrators of any staffing changes in a timely manner. On multiuser devices, file system access controls are implemented to ensure that data is not accessed by unauthorized users. Systems used to process or store Confidential or Restricted Use information do not host any unauthenticated service that allows access to browse the file system, such as anonymous ftp or directory indexing via a web server.

- Describe your technical and physical safeguards. Examples include:
  - Actions taken to physically secure data files, such as site and office access controls, secured file cabinets and locked offices.
  - Safeguards to limit access to CO APCD data and analytical extracts among the research team (Note: if the distribution of analytical data extracts among the researcher team is part of your data management plan, the extracts remain subject to the terms of your Data Use Agreement).

Servers storing significant quantities of Confidential data or any Restricted Use data are kept in secure rooms with strong physical access controls. Two factor physical access controls and video surveillance of these areas are in place. System/Device based firewalls are used where it is reasonable to do so, are recommended for systems with Confidential data, and required for systems with Restricted Use data. Sensitive Information is encrypted in transit where it is reasonable to do so using VPN, SSL, or similar technologies. Encryption in transit is strongly recommended for Confidential data and required for Restricted Use. Network-accessible systems that contain Restricted Use information from multiple individuals should require two-factor identification where technically practicable, including access by individuals to their own data.

- Provide a brief description of your policies and procedures for ensuring that CO APCD data are protected when stored on a server.
  - Describe how your organization prevents the copying or transfer of data to local workstations and other hard media devices (CDs, DVDs, hard drives, etc.). Note that Applicants are required to encrypt CO APCD data both in motion and at rest:

CO APCD data will be encrypted at rest on the server. 2 factor VPN authentication provides encryption in transit. The researchers will not transfer data files to local computer. All analytical output will be compliant with cell suppression policies outlined in the data use agreement, and local computers are encrypted and equipped with anti-malware software.

Restricted Use data must be encrypted at rest under Boston University's minimum security standards, in transit via a 2-factor verification VPN. (http://www.bu.edu/policies/minimum-security-standards/). Systems will be routinely scanned for vulnerabilities and discovered vulnerabilities will be remediated swiftly. Anti-virus software will be installed and tied to enterprise management and reporting utilities. Network services that do not have an associated business need will be disabled. Non-Endpoint devices

will be configured to sync time information (Network Time Protocol) from an established, credible source. Where possible, authentication to Non-Endpoint devices or software should be from approved enterprise authentication services (e.g. Active Directory, Kerberos, Shibboleth).

- Data Reporting and Publication
  - Your organization must ensure that all analytic extracts, analyses, findings, presentations, reports, and publications based on CO APCD data files adhere to specific requirements of the Data Use Agreement (DUA: refer to sections 6, 7 and 8 in the Data Use Agreement). **Briefly describe your plan for demonstrating that data reporting and publication processes will be consistent with the DUA, including adhering to CO APCD cell suppression policies:**

Since all data and all results will be stored on project space specific to this DUA, no results will be reported or released except after review by the PI for this DUA. The PI will be solely and personally responsible for ensuring that the requirements of this DUA are adhered to, including cell suppression policies. All reported data will be in aggregate with strict adherence to all cell suppression policies outlined in the DUA.

2. **Completion of Research Tasks and Data Destruction**

   Your organization must ensure that it has policies and procedures in place to destroy the CO APCD data files upon completion of the project and that you have safeguards to ensure the data are protected when researchers terminate their participation in the research project. Describe your plan for demonstrating that your organization has policies and procedures in place to reliably destroy the data files upon completion of the research:

In accordance with BUMC ITS policy, data covered by a DUA which stipulates its destruction shall be adhered to. BUMC IT will undertake erasure of all files associated with this project when informed by the PI or CO APCD data provider of the project's termination. Reusable media (disk drives) will be securely erased when removed from service. When Restricted Use data is involved, failed media that is not encrypted (even if under warranty) cannot be returned to the manufacturer if it cannot be wiped. These drives must be destroyed via our Media Destruction service. The form attached to this DUA as Appendix I will be filled in and transmitted to CO APCD data providers.

3. **Request for Privacy Board Approval** *(Only Applicable to Identifiable Data Requests)*

   Projects that request Identifiable information for a research purpose may require approval from the DRRC acting as a Privacy Board if an IRB is not available.

   - The DRRC, acting as a Privacy Board, may approve a waiver of the individual authorization normally required to release PHI under CFR § 164.508 if:
   - It would be impracticable for researchers to obtain written authorization from patients that are the subject of the research; and
   - The research could not practicably be conducted without access to and use of the PHI.
   - The DRRC, acting as a Privacy Board, is required to evaluate certain criteria in considering whether to approve an authorization waiver. If you are requesting Identifiable Information for a research purpose, explain why your proposed use of PHI involves no more than a minimal risk to the privacy of patients that are the subject of the research. Evidence of minimal risk to the privacy of patients that should be addressed in your explanation includes:

- An adequate plan to protect PHI identifiers from improper use and disclosure;
- An adequate plan to destroy PHI identifiers at the earliest opportunity; and
- Adequate written assurances that PHI will not be reused or disclosed.

Appendix I
Certification of Project Completion and Destruction or Retention of Data
(Please Save)

Name:	
Title:	
Organization:	
Address:	
Tel Number:	
Fax Number:	
E-mail Address;	
Project Title:	
Data Sets:	
Years:	
❒ Certification of Data Destruction	Date the Data was Destroyed:
❒ Request to Retain Data	Date Until Data Will Be Retained:

Instructions: 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).
I hereby certify that the project described in the Application is complete as of this date _____, ____, 20_.

Complete the appropriate section, below:

☐ I/we certify that we have destroyed all Data received from the CO APCD Administrator 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.

☐ I/we certify that we are retaining the data received in connection with the aforementioned project, pursuant to the following health or research justification (provide detail, use as much additional space as necessary and state how long the data will be retained).

☐ I/we hereby certify that we are retaining the Data received from the APCD Administrator in connection with the aforementioned project, as required by the following law. [Reference the appropriate law and indicate the timeframe].

By signing this Agreement, the Receiving Organization agrees to abide by all provisions set out in this Agreement.

SIGNATURES:

For the CO APCD:	**For Receiving Organization:**
Signature:	**Signature:**
Name: Pete Sheehan	**Name:** William P. Segarra, MA, JD, MPH
Title: VP of Client Solutions & State Initiatives	**Title:** Director, Contracts