CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

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:	22.50 Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace
Date:	December 6, 2021
Organization Requesting Data:	Duke University
Contact Person:	Katie Factor, JD
Title:	Strategic Services Associate, Senior Executive Vice Dean for Administration Office of Research Contracts Duke University School of Medicine
E-mail:	katie.factor@duke.edu
Phone Number:	(919) 681-5637 office
Person Responsible for the Project (if different than above):	Virginia Wang, PhD MSPH
Title:	Associate Professor Departments of Population Health Sciences and Medicine Duke University School of Medicine
E-mail:	virginia.wang@duke.edu
Phone Number:	(919) 668-1793 office; (919) 593-2832 personal mobile

Project Purpose:

Medicare's price setting strategies have potential to shape provider behavior. When Medicare prices are deemed too low, providers may close, stop caring for Medicare patients, or start to pursue other payer sources. Dialysis facilities, which care for patients with end-stage kidney disease (ESKD), are acutely impacted by changes in Medicare payment because Medicare offers near universal coverage for ESKD patients and has historically funded care for 90% of this patient population. Recent policy changes may have reportedly induced dialysis facilities to shift their payer mix – and thus patients' reliance on insurance coverage – away from Medicare, raising concerns about benefits and harms to patients and payers.

To date, there is no empirical evidence on whether dialysis facilities' shifts away from Medicare is being replaced with private insurance, or if specific types of patients are disproportionately affected by these changes. The US Renal Data System, the national registry for ESKD patients and providers, is limited in describing non-Medicare patients and revenue sources for dialysis facilities. All-payer data are necessary to fully describe the mix of insurance coverage among patients with ESKD on dialysis and to gather empirical evidence on the impact of changes in payer mix on patients' access to care, outcomes, and costs.

We propose to use the Center for Improving Value in Health Care (CIVHC) data to identify patient-level insurance coverage information across Medicare, Medicaid, and private insurance. We will address three questions related to dialysis patients in Colorado:

1. Did rates of Medicare and private insurance coverage among new ESKD patients change after federal policies impacting ESKD care payment and coverage?
2. What patient (e.g., demographic, clinical) and regional characteristics are associated with transition to enrollment in Medicare during the 1st year of incident ESKD?
3. Is patient's health insurance program associated with greater likelihood of home dialysis (modality of treatment that is less costly to providers and payers) and overall payments for dialysis within one year of initiation?

How will this project benefit Colorado or Colorado residents?
This study will conduct novel linkages of national disease registry and CIVHC's comprehensive payer data (e.g., traditional Medicare, Medicare Advantage, and non-Medicare sources such as Medicaid and commercial payers) to identify the policy implications of changes in health insurance coverage among Colorado's patients with kidney failure (e.g., costs, access to care).

Triple Aim criteria: How will your project support lowering health care costs?
Preliminary analysis of the national cohort of patients with incident ESKD found disproportionate shifts away from Medicare for patients who are not receiving publicly-financed insurance (i.e., many state Medicaid programs require patients with ESKD to enroll in Medicare). This would include patients who are uninsured without Medicaid, underinsured or have private insurance at dialysis initiation (e.g., employer-based, self-pay private insurance). For these patients, private insurance is obtained through third party charitable premium assistance for new policyholders or maintained among patients with employer-based insurance who become unemployed after dialysis initiation (via COBRA coverage). Compared to Medicare, this private insurance coverage may provide higher reimbursements to dialysis facilities.

The implications of these different sources of coverage for the cost burden of dialysis services for patients, state and federal government and taxpayers varies. It is unclear whether the purported diversion of patients from Medicare to private insurance increases overall spending (private and public) of ESRD.

Triple Aim criteria: How will you project help improve the health of Coloradans?
It is unclear whether and what benefits of shifts away from Medicare coverage extend to the care of patients with ESKD. Prior study findings generally have found that patients with private insurance have better dialysis-related outcomes. This study will extend the evidence base by assessing the extent to which Medicare vs non-Medicare enrolled Coloradans with ESKD have access to and receive home dialysis treatment modalities, which is commonly preferred by patients, associated with greater quality of life, and less costly to provider and payers.

Triple Aim criteria: How will your project improve the quality of care or patient experience?
It will be important to assess the extent to which Coloradans with ESKD are disproportionately affected by changes in insurance coverage. Patients are subject to insurance premiums (e.g., Medicare Part B or employer-based/COBRA private insurance premiums) and healthcare encounter cost-sharing (e.g., copayments, deductibles), and are therefore also sensitive to costs and cost-related access to care. In the case of ESKD patients may rely on assistance navigating coverage options and may not have full information when it comes to the extent of costs of their care.

Diversion away from traditional sources of healthcare coverage for ESKD may exacerbate patient disparities in access to insurance coverage. In addition to concerns about payer spending, inadvertent patient impacts have received little attention. This study will provide important patient context to shifts in ESRD payer mix, by identifying the characteristics of patients who are disproportionately affected by decreasing/delayed entry into Medicare and increasing enrollment in private health plans, and associated impacts on access to patient-centered treatment options and healthcare costs.

- **Type of data requested:** claims data set

- **Do you need Protected Health Information (PHI):**
  - Yes – full identifiable dataset for finder file (file #1)
  - No – finder-file linkable Level 3 de-identified dataset for analysis (file #2)

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

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 → with sequencing for analysis
☐ Limited Data Set*
☒ Identified Data Set * → for finder file use and linkage with US Renal Data System standard analytic files

*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 – Limited and Fully Identifiable Data Sets

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.

Overview and Justification: Requesting for merge of CIVHC data to US Renal Data System national disease registry of patients with end-stage kidney disease for insurance coverage ascertainment and outcomes analysis. Study team will facilitate administrative coordination of CIVHC and USRDS data merge, with data merge conducted between CIVHC and USRDS.

Therefore, this CIVHC Data Release Application requests authorizations for 2 CIVHC datasets:

1) Fully identifiable finder file: for identifying patients in the US Renal Data System (national end-stage renal disease registry) standard analytic file and CIVHC datasets. With CIVHC approval, USRDS allows for linkage to occur between USRDS and CIVHC and linkages conducted by USRDS.

2) Level 3 De-identified dataset: with the USRDS-CIVHC linking unique identifier

Type of Data	Justification for Elements on the DED
Names	Finder file use only (see explanation, above). • First name (text) • Last name (text)
Street Address	
City	
Zip Code	
Health Plan Beneficiary Numbers	Finder file use only (see explanation, above). • SSN (text, 9-digit including leading zeroes) or • HIC (text)
Dates (including Day and Month detail.) Specify which date fields are needed and why.	Finder file use only (see explanation, above). • Date of birth (numeric mmddyyyy if possible) • Date of death (numeric, mmddyyyy if possible)
Provider Identifying Information	
Additional data elements for linking to other datasets, if available:	
Sex: male or female	Finder file use only (see explanation, above).
Internal unique identifier	CIVHC assigned unique identifier that enables linkages of CIVHC de-identified dataset to US Renal Data System patient demographic and "baseline" clinical information

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?** Requesting the use of as many of the following USRDS-approved data elements for finder file / data linkage: SSN, Date of birth, First and Last Name, Sex, Date of death (if available)
- **Once the linkage is made, what non-CO APCD data elements will appear in the new linked file?** US Renal Data System Core, Standard Analytic files containing ESKD patient demographic, clinical characteristics, Medicare payer history, ESKD treatment history, and Medicare claims.
- Have all necessary approvals been obtained to receive and link with the other data files (e.g., IRB or Privacy Board approval)?

  ☒ Yes, if so please provide copy → IRB approval documentation attached,
  → USRDS Data Use Agreement in progress

  ☒ In progress, anticipated approval date: ___Anticipated Jan 2022_____

  ☐ No or N/A, reason: _____

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?** Anticipated dissemination to health services and policy communities:
    - Preliminary and final research findings submitted for presentations at national conferences (e.g., AcademyHealth, American Society of Nephrology),
    - manuscripts submitted for peer-reviewed publication (e.g., JAMA, Health Services Research)

  As per data use agreements with CIVHC and USRDS, the research team will comply with all requirements (review and pre-approval) for disseminating research findings in a manner that complies with privacy requirements.

- **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:** progress and final research reports to grant sponsors, Robert Wood Johnson and AcademyHealth, will still comply with privacy requirements of CIVHC and USRDS.

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:	US Renal Data System, National Institute of Diabetes and Digestive and Kidney Diseases
Contact Person:	Kevin Abbott, MD MPH
Title:	Program Director
Address:	6707 Democracy Blvd, Room 621 Bethesda, Maryland 20892
Telephone Number:	Direct: 301.594.7714 USRDS: 1.888.998.7737
E-mail Address:	Direct: kevin.abbott@nih.gov USRDS: usrds@usrds.org
Role or responsibility in this project	USRDS Contracting Officer Representative

Description: Requesting for merge of CIVHC data to US Renal Data System national disease registry of patients with end-stage kidney disease for insurance coverage ascertainment and outcomes analysis. Study team will facilitate administrative coordination of CIVHC and USRDS data merge, with data merge conducted between CIVHC and USRDS.

Project Schedule:

Proposed Project Start Date:	12/01/2021
Project End Date:	11/30/2022 (with extension possible)
Proposed Publication or Release Date:	Fall 2022 to Winter 2023
End of Date Retention Period:	5 years post publication (can limit data retention to final, de-identified analytic file, if needed)

D. Frequency

Data in the CO APCD Warehouse is refreshed every other month 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 be identified.

☒ 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.

Duke University Data Privacy and Security Policies and Procedures document is attached.

- **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.**

  To the best of our knowledge, no members of the project team have been involved with a project that experienced a data security incident.

  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:**

    The following data storage and confidentiality procedures are designed to maintain the confidentiality of potentially identifiable patient information.

    Duke Health Technology Solutions manages the servers and networks where the electronic study data (CO APCD data files) will be stored. DHTS has extensive electronic data safeguard procedures in place. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All media containing PHI are stored in a locked file cabinet in a room secured with limited electronic key access. All data are securely stored on servers that are behind the Duke firewall.

    The CO APCD data used for this project will be moved into the Duke Department of Population Health Sciences PACE environment. Data will be stored and analyzed on DHTS servers as described above, with access granted only to those with appropriate training, familiarity with the regulations for data use, and a need to know. Data use agreements for use of the CO APCD data will be fully executed prior to being granted access to the data set.

    All analysis of CO APCD data will be performed within PACE. PACE is the Protected Analytics Computing Environment at Duke and it provides a full function, high capacity environment for analyzing data. It is

a computation infrastructure behind the Duke Health firewall which is hosted by the Duke Data Centers and adheres to all of Duke's security protocols. PACE allows Duke researchers and external collaborators, where appropriate, to work together on projects using a common data warehouse. PHI is housed in an environment that meets best practice standards for data protection covering HIPAA, 21 CFR Part 11, and Federal Information Security Management Act (FISMA). Duke faculty, staff and collaborators' access to these data are managed and monitored by access control measures overseen by project leadership.

All data transactions within PACE can be monitored and audited. All computations can be run on the servers and no data can be removed from the serves and stored in other locations, except via an honest broker where the approved IRB protocol supports that transfer. Results from the analyses can be moved out of PACE, but must be reviewed by an honest broker to confirm that all PHI has been de-identified.

- **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:**

    The study investigators (V. Wang, B. Hammill, and C. Sloan) and statistical programmers and analysts (M. Stagner, N. Frascino, and L. Zepel) will have access to CO APCD data. Study data are on password-protected servers maintained by Duke University as described above. In addition, the Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users (including those listed above) are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall. No data will be transferred to the hard drive of a desktop/laptop computer. Access to PACE as a user is granted by adhering to a confidentiality agreement.

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

    Study data are on password-protected servers maintained by Duke University. No data will be transferred to the hard drive of a desktop/laptop computer. The study investigators (V. Wang, C. Sloan) and statistical analysts (N. Frascino and L. Zepel) will be the only study team members who will have access to the data in

the password-protected servers maintained by Duke University. In addition, the Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall. In addition, all staff with access to the data in the PACE environment will have had to complete PACE regulatory and training requirements.

- **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:**

  The project manager (J. Genova) and the study investigators (V. Wang, C. Sloan) will track the active status and roles of each member on the project. The project manager and/or study investigators will inform CO APCD of any changes to the project team within 30 days of the personnel change.

- **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.**

    All file and directory access is controlled by groups and users rights. All media containing PHI are stored in a locked file cabinet in a room secured with limited electronic key access. All data are securely stored on servers that are behind the Duke firewall. The CO APCD data used for this project will be integrated into the Department of Population Health Sciences PACE environment. Data will be stored and analyzed on Duke Health Technology Solutions servers as described above, with access granted only to those with appropriate training, familiarity with the regulations for data use, and a need to know. Data use agreements for use of the CO APCD data will be fully executed prior to being granted access to the data set.

  - **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).**

    Data will be stored and analyzed on Duke Health Technology Solutions servers as described above, with access granted only to those with appropriate training, familiarity with the regulations for

data use, and a need to know. Only the study investigators (V. Wang, B. Hammill, and C. Sloan) and statistical analysts (M. Stagner, N. Frascino, and L. Zepel) will have access to CO APCD 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 handled and analyzed at Duke University by approved study team members. We will extract data from the CO APCD files, abiding by terms set forth in the executable DUAs between Duke University and NIH-NIDDK /USRDS, and Duke University and CIVHC. Copies of the fully executed Data Use Agreement will be furnished before any data is transferred or accessed. Electronic data will only be transferred to other password-protected storage spaces (i.e., university-based server space). Only the investigators and data programmers indicated in executable IRB-approved protocols and DUAs will have access to storage and work with this data. The Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall.

- **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:**

    The study team has extensive experience executing data use agreements with similar data reporting and publication criteria, such that no person or organization are disclosed in reports or publications. Reported data is aggregated (i.e., combined into groups of data) and no cell sizes (aggregates of data) contain information on fewer than ten (10) individuals, and/or from which identities of individuals or organizations could be inferred. In accordance to data use agreements, manuscripts for

publication/reports are submitted to data sources (e.g., CIVHC, USRDS) for privacy review and approval prior to their submission.

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:

We anticipate completion of this project within 1-2 years of receipt of the data from CIVHC. This includes 12 months to clean and restructure data for data analysis, analytical modeling and specification, and final data analysis. The CO APCD data will be destroyed at the end of the project.

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.

CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

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:** Duke University
Signature:	**Signature:**
Name: Pete Sheehan	**Name: Katie Factor, JD**
Title: VP of Client Solutions & State Initiatives	**Title:** Strategic Services Associate, Senior Executive Vice Dean for Administration, Office of Research Contracts

Addendum I – Analyst Supplement
Colorado All Payer Claims Database Application

Project Description and Data Objective

Project Title and number: 22.50 Duke University: Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace

Objective: This study will conduct novel linkages of national disease registry and CIVHC's comprehensive payer data (e.g., Medicare Advantage, and non-Medicare sources such as Medicaid and commercial payers) to identify the policy implications of changes in health insurance coverage among Colorado's patients with kidney failure (e.g., costs, access to care).

***Data request – special note:** This CIVHC Data Release Application-Supplement requests authorization for 2 CIVHC datasets:

1. Fully identifiable finder file: for identifying patients in the US Renal Data System (national end-stage renal disease registry) standard analytic file and CIVHC datasets. With CIVHC approval, USRDS allows for linkage to occur between USRDS and CIVHC and linkages conducted by USRDS.
2. Level 3 De-identified dataset: with the USRDS-CIVHC linking unique identifier

Date Range or Years Requested – *What years of claims do you need to meet your project purpose? (If you want a range of data with specific month and day start and end dates, please supply the start and end dates next to the appropriate year.)*

requesting same years of data for
1) finder file (linked to eligibility months)
2) de-identified dataset (linked to member eligibility date and claim service date)

Check all that apply:

- ☒ 2012
- ☒ 2013
- ☒ 2014
- ☒ 2015
- ☒ 2016
- ☒ 2017
- ☐ 2018
- ☐ 2019
- ☐ 2020*

*Please consult the Data Warehouse refresh schedule to learn what is currently available for 2020

Medicare FFS data: Data requests are only available for research purposes and must be approved and financially supported by HCPF.

Check all that apply:

- ☐ 2012
- ☐ 2013
- ☐ 2014

☐ 2015
☐ 2016
☐ 2017
☐ 2018

Lines of Business: *Which payers do you need for your project purpose?*

Please check all that apply

☒ **Commercial Payer Claims** - Data available with appropriate levels of aggregation
Need to discuss appropriate level of aggregation for client request type; would need analyst input

☒ **Individual**

☒ **Small Group Plans**

☒ **Large Group Plans**

- ***Currently available:*** Medical Claims AND Pharmacy Claims from 2012-2020
  - **Claims**
  - **Eligibility**
  - **Servicing and Billing Provider information**

☒ **Fully insured Employer Plans**

☒ **Self-Insured ERISA and non-ERISA based Employer Plans (note: ERISA-based plans are voluntary submitters and are not all represented in the CO APCD)**

- ***Currently available:*** Medical Claims AND Pharmacy claims
  - **Claims**
  - **Eligibility**
  - **Servicing and Billing Provider information**

☒ **Medicare Advantage** - data is available with appropriate levels of aggregation
Need to discuss appropriate level of aggregation for client request type; would need analyst input

- ***Currently available:*** Medical AND Pharmacy claims from 2012-2020
  - **Claims**
  - **Eligibility**
  - **Servicing and Billing Provider information**

☒ **Health First Colorado (Colorado's Medicaid Program)** - Data requests must be reviewed by the Colorado Department of Health Care Policy and Financing (HCPF) to ensure alignment with administration of the Medicaid program as required by federal law

- ***Currently available:*** Medical Claims AND Pharmacy Claims from 2012-2020
  - **Claims**
  - **Eligibility**
  - **Servicing and Billing Provider information**

The following lines of business, when requested, require CIVHC Data Release Review Committee review as well as HCPF review, approval, and financial support.

☐ **Medicare Fee For Service (FFS) -** Data requests are only available for research purposes and must be approved and financially supported by HCPF.

- ***Currently available:*** Medical Claims AND Pharmacy Claims from 2012-2018

- **Claims**
- **Eligibility**
- **Servicing and Billing Provider information**

Payer-Specific Details – Do you need to limit claims to particular health insurance coverage types?

☐ **Yes**
☒ **No**

- **If YES,** please indicate the specific information you would like to include:
  - **Payer Line of Business**
    - ☐ **Commercial**
      - **Payer Name: Please note Anti-trust guidelines will be followed. (DRRC review maybe also be required)**
      - **Commercial Product Line(s):**
        - ☐ **PPO**
        - ☐ **HMO**
        - ☐ **POS**
        - ☐ **Supplemental**
        - ☐ **Indemnity**
        - ☐ **Other- Please specify**

    - ☐ **Colorado's Exchange, Connect for Health Colorado, Product Lines**:
      - ☐ **Gold**
      - ☐ **Silver**
      - ☐ **Bronze**

Payment Type – *Which elements of total paid amount on each claim do you need to support your project purpose? (Check all that apply)*

☒ **Charged Amount**
☒ **Plan Paid Amount***
☒ **Member Liability, i.e., amount the member is responsible for (check all that apply)**
  - ☒ **Coinsurance**
  - ☒ **Deductible**
  - ☒ **Copay**

☒ **Total Allowed Amount** – (summation of plan paid and member liability)
☒ **Prepaid Amount** – (*to be considered for capitated payment plans only*)

Medical Claims – *Which types of claims do you need for your project purpose? (Check all that apply)*

☒ **Inpatient (IP)** – Related to individuals who receive care in hospital settings
☒ **Outpatient (OP)** – Related to an individual receiving medical treatment in any setting other than a hospital admission (i.e. ambulatory surgery center; doctor's office, imaging center, Emergency Room, home health, etc.)

☒ **Professional (PROF)** – Related to medical procedures within professional settings (e.g. physician office, imaging center, etc.) and clinics

Pharmacy Claims – *Do you need prescription drug-based claims for your project purpose?*

☒ **Yes**
☐ **No**

- **If YES**, and you need pharmacy claims limited to specific drug types, ***please list the 11-digit NDC codes you would like to receive (DO NOT INCLUDE DASHES AND PROVIDE LEADING ZEROS):***

Dental Claims – *Do you need dental claims for your project purpose?*

☐ **Yes**
☒ **No**

Site of Service Detail – *Do you need to look at claims that occurred in specific care settings for your project purpose? i.e., do you need to limit services by site of service?*

☐ **Yes**
☒ **No**

- **If YES,** please indicate the specific information you would like to include:
  - ☐ **Hospital**
  - ☐ **Ambulatory Surgery Centers**
  - ☐ **Outpatient Facilities**
  - ☐ **Physician offices**
  - ☐ **Specialty offices**
  - ☐ **Home Health**
  - ☐ **Urgent Care**
  - ☐ **Emergency Room (Note: cannot differentiate between majority of Free-Standing and hospital-based ERs)**
  - ☐ **Other** (specify)

Provider-level Detail – *Do you need claims limited to specific providers or provider type(s) ie. (Provider IDs, locations, hospitals, medical groups, etc.) for your project purpose?*

☐ **Yes**
☒ **No**

- **If YES,** please indicate the specific provider types you would like to include or provide a list of providers:
  - ☐ **Facilities (hospitals, ambulatory surgery centers, etc.)**
  - ☐ **Professionals**
  - ☐ **Provider Taxonomy - Specialty Designations**
  - ☐ **National Provider Identifier**
  - ☐ **Other**

Geography– *Do you need claims data limited by geography or location for your project purpose?*

☐ **Yes**
☒ **No**

- **If YES,** please indicate the geographic groupings you would like to include:
  - ☐ **Provider location address**
  - ☐ **Member location address**
  - ☐ **Zip 3**
  - ☐ **Health Statistic Region**
    http://www.cohid.dphe.state.co.us/brfssdata.html
  - ☐ **County (Potential PHI)**
  - ☐ **Zip 5 (PHI)**
  - ☐ **Other**

Age and/or Gender – *Do you need claims data limited by age or gender for your project purpose?*

- ☐ **Yes**
- ☒ **No**

- **If YES,** please indicate the groupings you would like to include:
  - ☐ **Age bands/range (in years) requested (i.e. 0-21, 22-39, 40-55, etc.)**
  - ☐ **Gender**
    - ☐ **Male**
    - ☐ **Female**
    - ☐ **Unspecified**

Member-level Detail – *Do you need claims filtered at the member level for your project purpose? i.e., do you need claims limited to specific members for your project?*

[NOTE: responses in this section refer to the finder file data request only]***

- ☒ **Yes**
- ☐ **No**

- **If YES,** please indicate the information you would like to include:
  - ☒ **De-identified member information**
    - ☒ **Unique member and person ID**
    - ☒ **Gender**
    - ☐ **Age: (at time of service)**
    - ☐ **3-digit zip**
  - ☒ **Protected Health Information (PHI)** – Any of the below requires DRRC approval process
    - ☒ **Names (first, last, middle) (PHI)**
    - ☐ **Street Address (PHI)**
    - ☐ **City (PHI)**
    - ☒ **5 Digit Zip (PHI)**
    - ☒ **DOB-Dates of Birth (PHI)**
    - ☒ **DOS-Dates of Service (PHI)**

Diagnosis Detail – *Do you need claims limited to a specific diagnosis or multiple diagnoses for your project purpose?*

☐ **Yes**
☒ **No**

[NOTE: Understanding that there could be patients in the USRDS file who do not have a corresponding diagnosis code in the CO APCD, the study team requests attempt to link all members from the CO APCD eligible during the study timeframe without limiting by dx code. In the event that this request is computationally burdensome or poses data security concerns, the study team would alternatively request sending a finder file for linkage based on all CO APCD members with EVER any of the following diagnosis codes, specified below.]***

- **If YES,** please indicate the specific diagnosis code(s) you would like to include (DO NOT USE DECIMAL POINTS AND DO NOT REMOVE LEADING AND TRAILING ZEROS):
  - *ICD9: 5855 (CKD stage 5)*
  - *ICD9: 5856 (ESRD)*
  - *ICD10: N185 (CKD stage 5)*
  - *ICD10: N186 (ESRD)*
  - *ICD10: N19 (unspecified kidney failure)*

Procedure/Revenue Code Detail – *Do you need claims limited to specific procedure or revenue code(s) for your project purpose?*

☐ **Yes**
☒ **No**

- **If YES,** please indicate the specific procedure/revenue code(s) you would like to include under each type requested:
  - ☐ **CPT4**
  - ☐ **CDT**
  - ☐ **Revenue code**
  - ☐ **APR-DRG**
  - ☐ **ICD9 or ICD10**
    (Please indicate whether the codes you provide are ICD 9 or 10 codes)

Additional Requests/Info Not Included Above – Clarification on requested data files

Requesting for merge of CIVHC data to US Renal Data System national disease registry of patients with end-stage kidney disease for insurance coverage ascertainment and outcomes analysis. Study team will facilitate administrative coordination of CIVHC and USRDS data merge, with data merge conducted between CIVHC and USRDS.

Therefore, this CIVHC Data Release Application requests authorizations for 2 CIVHC datasets:

1. Fully identifiable finder file: for identifying patients in the US Renal Data System (national end-stage renal disease registry) standard analytic file and CIVHC datasets. With CIVHC approval, USRDS allows for linkage to occur between USRDS and CIVHC and linkages conducted by USRDS.

USRDS allows the following identifiers to be used to merge data, for CIVHC to use/apply when available:

- An internal unique identifier (crosswalk patient identifier, assigned by CIVHC)
- SSN (text, 9-digit including leading zeroes) or HIC (text)
- Date of birth (numeric mmddyyyy if possible)
- First name (text)
- Last name (text)
- Sex (character, M or F)
- Date of death

After merging the CIVHC finder file with the USRDS database, the USRDS Coordinating Center will return to

a) CIVHC a crosswalk file containing the unique identifier provided and the USRDS ID for all identified individuals. (USRDS does not provide nor return unique patient identifiers.)

b) the Duke University-based study team a crosswalk file of USRDS ID and the CIVHC-linking unique identifier

2. Level 3 De-identified dataset: with the USRDS-CIVHC linking unique identifier

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:** Duke University
Signature:	**Signature:**
Name: Pete Sheehan	**Name: Katie Factor, JD**
Title: VP of Client Solutions & State Initiatives	**Title:** Strategic Services Associate, Senior Executive Vice Dean for Administration, Office of Research Contracts

Data Classification Standard [1]

Version 2.2

Author

University IT Security Office (ITSO)

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Definitions

TERM	DEFINITION
Data Steward	The individual who has accountability and executive authority to make decisions about a specific set of data. The Data Steward is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.

Data Manager	The persons who are responsible for implementing the controls the Data Steward identifies.
Data Users	The persons who actually "touch" the information (enter, delete, even read).
Protected Data	Any information classified as either Sensitive or Restricted by the Duke standard.

Purpose

While performing their assignments at Duke University, all users will likely come into contact with many types of information or data, some of which may be considered Sensitive or Restricted according to Duke’s data classifications and regulatory requirements. It is the responsibility of Duke to implement procedures and standards to help users protect their data.

The purpose of this standard is to define Duke’s data classifications and data types for each classification. Please be aware that applicable federal and state statutes and regulations that guarantee either protection or accessibility of certain data records will take precedence over this standard. These regulations and laws include:

- FERPA (which protects many kinds of student educational data)
- HIPAA (which protects personal health information)
- HHS Title 45 CFR Part 46 - Protection of Human Subjects (which applies to research supported by a federal agency)
- NC GS 125-19 (which protects the privacy of library patrons' records)
- NC Identity Theft Protection Act (which defines personal information and requires notification if a data breach occurs)
- PCI (which protects credit card holder information)

Scope

This standard applies to all data collected, stored, or processed by university staff or by third parties via contractual agreements with university departments or other organizational groups.

Standards

Data and Risk Classifications

To assist in handling information in any format, Duke as defined three classes of information: Sensitive, Restricted, and Public. Each classification tier requires a specific level of technical and procedural security controls due to the risk impact if the information is mishandled. These Technical Standards may be found here [2].

Data that has not yet been classified should be considered Restricted until the Data Steward assigns the classification.

The classification of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as Sensitive. If paper credit card receipts are stored, then they should be classified as Sensitive.

Questions about classifying or handling the data should be directed to the Data Steward, your supervisor, your departmental security liaison, or the University IT Security Office. The departmental security liaisons, in coordination with the IT Security Office, can assist departmental users in developing appropriate controls and processes to protect Sensitive or Restricted data.

Data Category & Risk	Definition & Access	Examples

Sensitive (High)	Sensitive data is the most restrictive data classification category and is reserved for data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. Explicit institutional approval is needed in order to receive access to Sensitive data.	• Social Security numbers [3] • Credit Card numbers [4] • PHI (HIPAA - protected data) • FERPA-protected data (non-directory information) • Prospective student data • Donor data • CUI (controlled unclassified information) • Contract data • Financial data • HR data • Physical Plant details • Research data • Certain management information
Restricted (Medium)	Restricted information is the default data classification category. Restricted data is data that is not necessarily for public consumption, but also does not fit into the Sensitive category. Duke may have a proprietary obligation to protect Restricted data, but disclosure would not significantly harm the university. Access to Restricted data elements is determined by business process needs.	• Anything not Public or Sensitive • Data that is restricted to specific groups • Research detail that is not classified as Public or Sensitive • Library transactions • Financial transactions not including Sensitive data • NDA data

Public (Low)	All other data, which can be accessible to the general public. Information that has been approved for publication, such as a press release or information published on www.duke.edu [5]. (This does not include information that has been disclosed accidentally.) Access includes Duke University affiliates and general public.	• Public-facing websites • Campus Maps • FERPA directory data • Faculty/Staff directory data • Research data

Roles and Responsibilities

To handle data properly, Duke faculty and staff need to be aware of the classification of a piece of information and the associated risks in order to understand how to properly and securely handle the information.

TERM	DEFINITION
Data Steward	The individual who has accountability and executive authority to make decisions about a specific set of data. The Data Steward is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.
Data Manager	The persons who are responsible for implementing the controls the Data Steward identifies. The data managers are responsible for ensuring that the appropriate security controls are in place on systems containing Sensitive and Restricted data (see Technical standards).
Data Users	The persons who actually "touch" the information (enter, delete, even read). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Steward.

Campus Units	It is the recommendation of the Duke University IT Security Office that all campus units that collect and store information document their policies, procedures, and architectures that pertain to collection and storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures.

Sensitive Server Registration

The University IT Security Office tracks servers containing Sensitive data. Campus units are asked to document which of their servers contain Sensitive and Restricted data, and update the ITSO on which systems contain Sensitive information.

Incident Reporting

Report the misuse or compromise of systems that handle, store, or propagate Sensitive data IMMEDIATELY to security@duke.edu [6].

Review Frequency: Annually

Updated: 07/14

In Compliance with:
Duke University Technical Standards [2]
Duke University Acceptable Use Policy [7]

Document Type: Policy **Topic:** Data Security **Applicable To:** Duke Health, Duke University

Links
[1] https://security.duke.edu/policies/data-classification-standard
[2] https://security.duke.edu/policies-standards-procedures?keys&document_type_value=2&topic_tid=All&duke_dept_value=All
[3] https://security.duke.edu/policies/social-security-number-usage-policy
[4] https://finance.duke.edu/banking/ecommerce/reginfo
[5] http://www.duke.edu
[6] mailto:security@duke.edu
[7] https://security.duke.edu/policies/acceptable-use

Data Security Policy [1]

Version 1.1

Authority

Duke University Chief Information Officer
Duke Health Chief Information Officer
Duke University Chief Information Security Officer
Duke Health Chief Information Security Officer

Purpose

As stewards of Duke's resources, we are expected to exercise sound judgment using data prudently and ethically. Additionally, various federal and state laws impose obligations on Duke, including, but not limited to HIPAA [2], FERPA [3], FISMA, the NC Identity Theft Protection Act and PCI-DSS [4]. Grants and contracts may impose requirements for the protection and preservation of associated data. As a result, it is important that all data (with appropriate priority given to Sensitive and Restricted data[1]), are reasonably and appropriately managed to maintain data integrity, availability, and when required, confidentiality to protect against accidental or unauthorized access, modification, disclosure and destruction.

Special consideration to research data is warranted, as some research data may be classified as public and open, while other research data may require greater protections due to the sensitivity of the data. This policy is not intended to impede the use or sharing of unrestricted (e.g. public) research data, but rather provide the framework for determining where controls are required for sensitive or protected research.

While every reasonable effort has been made to document the appropriate protections and responsibilities for data, it is possible that a specific case or issue may not be addressed or may raise a question. In such a case, the department or user is strongly encouraged to reach out to the appropriate security office (see Data Procedures section) for assistance determining the appropriate course of action.

Policy

Data Classification

Each user is responsible for knowing Duke's data classification standard and the associated risks in order to understand how to classify and secure data. Duke data classifications are Sensitive, Restricted or Public. Sensitive data requires the highest level of security controls, followed by Restricted and then Public. A link to the Duke Data classification standard is provided in Appendix B.

Data Access & Usage

Consistent with its classification, data shall be accessible to authorized users to fulfill their duties and responsibilities.

Data Maintenance & Disposal

A user with authorized access to data will maintain the security (confidentiality, integrity and availability) of the data, consistent with Duke requirements. When Sensitive and Restricted data must be disposed of, to the extent permissible under law, that disposal must be in a manner that renders it unrecoverable. Only authorized services can be used for storage of Duke sensitive data; an approved list is available online: https://security.duke.edu/policies/duke-services-and-data-classification [5]. Should you have questions about use of a service to store sensitive data, we encourage you to contact the Security Offices at security@duke.edu [6].

Data Encryption

Sensitive data must be encrypted during network transmission, and if stored on mobile devices or removable media like a USB thumb drive. Any exceptions must be documented via a ServiceNow ticket and filed with the Duke IT Security Office or Duke Health Information Security Office for review. Additional information on encryption requirements for campus departments may be found here [7], while additional guidance for Duke Health may be found here.

Data Procedures

All Data Stewards at Duke must document their procedures, and other requirements that pertain

to the security of the data for which they are responsible. This documentation must comply with all Duke standards regarding data. The university Information Technology Security Office and Duke Health Information Security Office can be reached at security@duke.edu [6].

Incidents

Any security incident or suspected security incident involving a Duke system, especially those containing Sensitive or Restricted data, must be reported immediately to the University IT Security Office or Duke Health Information Security Office, Data Manager and Data Steward, as applicable, pursuant to the incident management procedures referenced in Appendix B.

Violations

Any violation of federal or state law, or this or other applicable policies, standards or contracts may result in corrective action up to and including dismissal/termination.

Responsibilities

Set forth in Appendix A are typical responsibilities for the executive officers for Duke University and Duke Health, Data Stewards, Data Owners, Data Managers and users. An individual may fulfill the responsibilities of more than on position. Data stewards and data managers also qualify as users with regard to fulfilling their duties and responsibilities on behalf of Duke.

Scope

This policy is intended to safeguard all data, with priority given to Sensitive and Restricted data.

This policy applies to all trustees, senior officials, faculty, staff, students, subcontractors, or other persons who may have access to Duke data. See **Definitions** below.

This policy applies to all data on Duke's communications resources, whether those resources are individually controlled, shared, stand-alone, or networked. It applies to all computers (including mobile devices) and communications facilities owned, leased, operated, or provided by Duke, or that are otherwise connected to Duke's communications resources. This policy also applies to all personally owned devices used to store, process, or transmit Duke data.

Definitions

Term	Definition
Data	Any items of information that are received, created, collected, maintained, accessed, provided by a third party (e.g., as part of a sponsored research project or other collaboration) and used, transmitted or disclosed for the fulfillment of the mission of Duke, whether in electronic, paper or other format.
Data Steward	The individual who has accountability and authority to make decisions about a specific set of data, and is responsible for defining the access and protection rules for a specific set of data.
Data Manager	The individual who is responsible for maintaining security controls to protect data established under law and by this and any other Duke requirements.
FERPA	Family Educational Rights and Privacy Act. The policy permits students to inspect their education records, limits disclosure to others of personally-identifiable information from education records without students' prior written consent, and provides students the opportunity to seek correction of their education records where appropriate.
FISMA	Federal Information Security Management Act. Mandates security for information systems subject to federal contracts.
HIPAA	Health Insurance Portability and Accountability Act. Restricts the release of health-related data about individuals. The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information.
NC ITPA	North Carolina Identity Theft Protection Act. Requires protection of individually identifiable data and mandates notification of individuals in the case of breaches and disposal of unneeded personal information.

PCI-DSS	Payment card industry data security standards. Rules for limiting access to financial information.
Security Incident	An adverse event in an information system. An incident may include a violation of an explicit or implied security policy, attempt to gain unauthorized access, unwanted denial of resources, unauthorized use, or changes without the owner’s knowledge, instruction or consent.
User	The individual who creates, accesses, processes, enters, reads, deletes or otherwise "uses" data.

APPENDIX A: Roles and Responsibilities

The duties and responsibilities listed below are provided to safeguard all data, with priority given to Sensitive and Restricted data, consistent with the fulfillment of Duke’s mission.

Executive Officers

The Executive Officers of Duke University and Duke Health who have oversight responsibility for establishing guidance and strategies for the protection of data through the Information Security Steering Committee (ISSC) and the Duke Health Privacy and Security Steering Committee (PSSC), and may delegate their implementation to the appropriate data steward(s).

Data Steward

A data steward is typically responsible for:

a. Classifying data in accord with the data classification standard.
b. Apprising the applicable Chief Information Security Officer of material issues related to the implementation of this policy.
c. Maintaining the accuracy and completeness of data for which they are responsible whether that data is contained in a centrally managed system or in a locally managed system.
d. Documenting and evaluating controls to maintain security, confidentiality, integrity, availability, and access of/to data that is in the custody of the data steward.

e. Designating a data manager(s) to implement security controls for the data in the custody of the data steward and providing necessary guidance and management assistance to the data manager(s).
f. Communicating data protection procedures to each data manager and user who is granted access to data in the custody of the data steward.
g. Monitoring compliance with applicable law, and with Duke policies, standards or contracts.
h. Facilitating consensus on data definitions, data usage, etc.
i. Fulfilling the principles and requirements set forth in this policy.

Data Manager

A data manager is typically responsible for:

a. Apprising the data steward of material issues related to the implementation of this policy.
b. Collaborating with the University IT Security Office or Duke Health Information Security Office, as necessary, to implement directives assigned by the data steward.
c. Ensuring that security controls are in place on systems containing Sensitive and Restricted data.
d. Data backup and recovery.
e. Being aware of relevant laws and of applicable Duke policies, standards or contracts.
f. Detecting and responding to violations and vulnerabilities.
g. Fulfilling the principles and requirements set forth in this policy.

User

In addition to the duties and responsibilities described in the policy, a user is typically responsible for:

a. Identifying, on a regular basis, data that qualifies as Sensitive or Restricted and reporting its existence to the appropriate data manager.
b. Following the security controls established by the data steward or data manager, as applicable.
c. Maintaining the security of data in her/his possession or control appropriate for the classification level of such data.
d. Avoiding disclosure of Sensitive or Restricted data to any unauthorized person without the documented permission of the data steward or manager.
e. Fulfilling the principles and requirements set forth in this policy.

Appendix B: References and Links

Acceptable Use Policy [8]
Account or Data Access Policy [9]

Application Risk Assessment [10]
DMCA [11]
Duke University Vulnerability Management Policy [12]
Duke HR Payroll Data Policy: http://www.hr.duke.edu/forms/secure/hrdata_policy.php [13]
Duke Corrective Action Policy:
http://www.hr.duke.edu/policies/expectations/standards/corrective_action... [14]
Duke Data Classification Standard [15]
Faculty Handbook: http://provost.duke.edu/faulty-resources/faculty-handbook [16]
FERPA: http://registrar.duke.edu/student-records [3]
FISMA: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf [17]
HIPAA: http://www.hhs.gov/ocr/privacy/ [18]
Human Resource Policies: https://www.hr.duke.edu/policies/ [19]
Incident Management Procedures [20]
NC Identity Theft Protection Act:
http://www.ncga.state.nc.us/sessions/2005/bills/senate/html/s1048v6.html [21]
PCI-DSS: https://www.pcisecuritystandards.org/security_standards [22]
Policies for the Responsible Conduct of Research: https://ors.duke.edu/orsmanual/policies-responsible-conduct-research [23]
Policy on Social Security Number Usage [24]
(Campus) http://security.duke.edu/sites/default/files/documents/DUHS%20SSNs%20201... [25]
(Health System)
Staff Handbook: http://www.hr.duke.edu/policies/staff_handbook.pdf [26]

---

[1]As defined in the Duke Data Classification Standard located here [15].

Review Frequency: Annually

Updated: 09/13
Updated: 05/14
Updated: 10/15

In Compliance with:
Duke University Acceptable Use Policy [8]

Document Type: Policy**Topic:** Data Security**Applicable To:** Duke Health
Source URL: https://security.duke.edu/policies/data-security
Duke University

Links
[1] https://security.duke.edu/policies/data-security
[2] https://www.dukehealth.org/patients-and-visitors/patient-bill-of-rights

[3] http://registrar.duke.edu/student-records
[4] https://www.pcisecuritystandards.org/pci_security/
[5] https://security.duke.edu/policies/duke-services-and-data-classification
[6] mailto:security@duke.edu
[7] https://security.duke.edu/policies/encryption-standard
[8] https://security.duke.edu/policies/acceptable-use
[9] https://security.duke.edu/policies/account-or-data-access-policy
[10] https://security.duke.edu/vendor-risk-assessment
[11] https://security.duke.edu/copyrightdmca
[12] https://security.duke.edu/policies/vulnerability-management
[13] http://www.hr.duke.edu/forms/secure/hrdata_policy.php
[14] http://www.hr.duke.edu/policies/expectations/standards/corrective_action.php
[15] https://security.duke.edu/policies/data-classification-standard
[16] http://provost.duke.edu/faulty-resources/faculty-handbook
[17] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[18] http://www.hhs.gov/ocr/privacy/
[19] https://www.hr.duke.edu/policies/
[20] https://security.duke.edu/services/incident-management
[21] http://www.ncga.state.nc.us/sessions/2005/bills/senate/html/s1048v6.html
[22] https://www.pcisecuritystandards.org/security_standards
[23] https://ors.duke.edu/orsmanual/policies-responsible-conduct-research
[24] https://security.duke.edu/policies/social-security-number-usage-policy
[25] https://security.duke.edu/sites/default/files/documents/DUHS%20SSNs%202011.pdf
[26] http://www.hr.duke.edu/policies/staff_handbook.pdf

DUHS INSTITUTIONAL REVIEW BOARD DECLARATION OF EXEMPTION FROM IRB REVIEW

The DUHS IRB has determined that the following protocol meets the criteria for a declaration of exemption from further IRB review as described in 45 CFR 46.101(b), 45 CFR 46.102 (f), or 45 CFR 46.102 (d), satisfies the Privacy Rule as described in 45 CFR 164.512(i), and satisfies Food and Drug Administration regulations as described in 21 CFR 56.104, where applicable.

Protocol ID: Pro00109690
Reference ID: Pro00109690-INIT-1.0
Protocol Title: Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace
Principal Investigator: Virginia Wang
Review Date: December 02, 2021
Expiration Date: **Does not expire*
Exempt Category: Category 4: Secondary research for which consent is not required: Secondary research uses of identifiable private information or identifiable biospecimens, if at least one of the following criteria is met: i. The identifiable private information or identifiable biospecimens are publicly available; ii. Information, which may include information about biospecimens, is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects; iii. The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR parts 160 and 164, subparts A and E [HIPAA], for the purposes of "health care operations" or "research" as those terms are defined at 45 CFR 164.501 or for "public health activities and purposes" as described under 45 CFR 164.512(b); or iv. The research is conducted by, or on behalf of, a Federal department or agency using government-generated or government-collected information obtained for nonresearch activities, if the research generates identifiable private information that is or will be maintained on information technology that is subject to and in compliance with section 208(b) of the E-Government Act of 2002, 44 U.S.C. 3501 note, if all of the identifiable private information collected, used, or generated as part of the activity will be maintained in systems of records subject to the Privacy Act of 1974, 5 U.S.C. 552a, and, if applicable, the information used in the research was collected subject to the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 et seq.

*This Declaration of Exemption from further IRB Review is in effect from December 02, 2021 and does not expire. However, changes to the proposed research will require an amendment requesting re-review for exemption. Reportable serious adverse events and unanticipated problems related to the research that place subjects or others at risk of physical, psychological, economic, or social harm must be promptly reported to the IRB and will result in reconsideration of the activity's exempt status.

DUHS Institutional Review Board
2424 Erwin Rd | Suite 405 | Durham, NC | 919.668.5111
Federalwide Assurance No: FWA 00009025

DUHS IRB Application (Version 1.0)

General Information

***Please enter the full title of your protocol:**

Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace

***Please enter the Short Title you would like to use to reference the study:**

ESKD Medicare Reliance After the ACA in Colorado
* This field allows you to enter an abbreviated version of the Study Title to quickly identify this study.

Add Study Organization(s):

List Study Organizations associated with this protocol:

Primary Dept?	Department Name
○	**DUHS** - - Margolis Center Operations
◆	**DUHS** - - Population Health Sciences

Assign key study personnel (KSP) access to the protocol

*** Please add a Principal Investigator for the study:**

(Note: Before this study application can be submitted, the PI MUST have completed CITI training)

Wang, Virginia

3.1 If applicable, please select the Key Study personnel: (Note: Before this study application can be submitted, all Key Personnel MUST have completed CITI training)
*** Denotes roles that are not recognized in OnCore. Please select an appropriate role that is recognized in all clinical research applications (iRIS, OnCore, eREG, etc.)**

A) Additional Investigators, Primary Study Coordinator (CRC), and the Primary Regulatory Coordinator (PRC):

Genova, Jessica
Primary Study Coordinator (CRC/CRNC/RPL)

B) All Other Key Personnel

***Please add a Study Contact:**

Genova, Jessica

Wang, Virginia

The Study Contact(s) will receive all important system notifications along with the Principal Investigator. (e.g., The study contact(s) are typically the Principal Investigator, Study Coordinator, and Regulatory Coordinator.)

Oncore

Please select the Library for your Protocol:

This field is used in OnCore. Determines the Reference Lists, Forms, Protocol Annotations, Notifications, and Signoffs available for the protocol. Protocols that require reporting to the NCI (National Cancer Institute), must select the Oncology library.

- ○ Oncology
- ◉ Non-Oncology

Protocol Application Type

Select the type of protocol you are creating:

Please see additional criteria and information in the policy titled "Reliance on the IRB of Another Institution, Organization, or an Independent IRB" on the **IRB web site**.

- ○ Regular Study Application - Most common. The IRB will determine if the study is eligible for expedited review or requires full board review upon submission.
- ◉ Application for Exemption from IRB Review - Includes Exempt, Not Human Subject Research, & Not Research.
- ○ External IRB Application - Any study using an external IRB as the IRB-of-Record.
- ○ Trainee Research While Away from Duke - Research conducted by medical students overseen by the Office of Curriculum & other student/trainee research away from Duke.
- ○ Individual Patient Expanded Access, Including Emergency Use - Use of an investigational product under expanded access, including emergency use of an investigational drug or biologic or emergency use of an unapproved device.

Oversight Organization Selection

CRU (Clinical Research Unit) or Oversight Organization Selection:

Please select the CRU.

Population Health Sciences

The Clinical Research Unit that takes responsibility for this study.

- Please select **Medicine** as the CRU **only** if the PI is in one of these Divisions or Institutes: Endocrinology, Gastroenterology, General Internal Medicine, Geriatrics, Hematology, Infectious Diseases, Nephrology, Pulmonary, Rheumatology & Immunology, Center for Applied Genomics and Precision Medicine, Center for the Study of Aging and Human Development, Duke Molecular Physiology Institute.
- More information on CRUs can be found on the Duke Office of Clinical Research (DOCR) website, **http://docr.som.duke.edu**
- Questions concerning CRU selection should be directed to docr.help@dm.duke.edu.
- For questions about the Campus Oversight Organization, please visit **Campus Oversight Organization**.

List all Key Personnel on the study who are outside Duke:

- **Note:** You will also need to attach the documentation of Human Subjects Certification for each individual, if they have completed the certification somewhere other than Duke.
- **If outside key personnel will have access to Duke PHI, a data transfer agreement AND external site IRB approval (or IRB authorization agreement) will be needed.** See HRPP policy **Use of Research Data by Former Duke Students or Former Duke Faculty and Employees**
- In the panel below, "PHI" is Protected Health Information.

Entry 1

Name	
Study Role	
Email Address	
Institution / Organization	
Will he/she have access to Duke P.H.I.?	○ Yes ○ No
Is he/she an unpaid volunteer at Duke on the study?	○ Yes ○ No

Sponsor and Funding Source

Add all funding sources for this study:

View Details	Sponsor Name	Sponsor Type	Contract Type:	Project Number	Award Number
⊟	Robert Wood Johnson Foundation	Institutional	Grant		78960

Sponsor Name:	Robert Wood Johnson Foundation
Sponsor Type:	Institutional
Sponsor Role:	Funding
Grant/Contract Number:	78960
Project Period:	From:12/01/2021 to:11/30/2022
Is Institution the Primary Grant Holder:	Yes
Contract Type:	Grant
Project Number:	
Award Number:	78960
Grant Title:	Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace
PI Name: (If PI is not the same as identified on the study.)	
Explain Any Significant Discrepancy:	

Is this a federally funded study?

○ Yes ◉ No

Does this study have any of the following?

- Industry sponsored protocol
- Industry funded Duke protocol
- Industry funded sub-contract from another institution
- Industry provided drug/device/biologic
- SBIR/STTR funded protocol

○ Yes ◉ No

As part of this study, will any samples or PHI be transferred to/from Duke to/from anyone other than the Sponsor, a Sponsor subcontractor, or a Funding Source?

◉ Yes ○ No

Is the Department of Defense (DOD) a funding source?

○ Yes ◉ No

Have you successfully synced your protocol to OnCore by clicking the 'Sync Data Over API' button at the top of this page?

Please verify that the protocol has been created in OnCore before submitting this application for PI Signoff.

◉ Yes, I synced my protocol to OnCore and verified it was successfully sent by logging into OnCore.
○ I may have forgotten! I'll click it again right now, just to be sure, and verify it was successfully sent by logging into OnCore.

Mobile Devices and Software

Does this study involve the use of a software or a mobile application?

○ Yes ◉ No

List all software, including third party (non-Duke) and mobile apps, that will be utilized for ascertainment, recruitment, or conduct of the research/project: (eg, MaestroCare, DEDUCE):

N/A.

Exempt Application

Project Summary:

Note: Data generated from an exempt project cannot be used in support of an FDA application for a drug/device/biologic. If you plan to utilize this data in support of an

FDA application, please do not continue with this exemption request and, instead, submit using the Regular Study Application pathway.

*Will you use data generated from this project to support an FDA application for a drug/device /biologic?.

○ Yes ◉ No

State the objectives of the research/project:

Medicare finances near-universal health care coverage for US patients with end-stage kidney disease (ESKD), regardless of age. Dialysis facilities, which treat the majority of patients with ESKD, are acutely sensitive to Medicare payment changes. When Medicare reimbursements are deemed too low, facilities may close, stop caring for Medicare patients, or pursue other revenue (payer) sources. In 2011, Medicare shifted away from fee-for-service and toward a bundled payment for dialysis services that decreased payment for some dialysis drugs and overall revenues for dialysis care[1] making patients covered by Medicare less profitable for dialysis facilities.

Medicare's payment change created incentives for dialysis facilities to increase their share of patients with private insurance, which reimburses dialysis facilities at significantly higher rates than Medicare. Charitable premium assistance programs, which are funded in part by dialysis provider organizations, have enabled some patients with ESKD to remain privately insured after becoming eligible to transition to Medicare. The 2014 Affordable Care Act (ACA) rules disallowing preexisting condition exclusions and the creation of ACA Marketplace for purchasing private insurance expanded the availability of private coverage.

In combination, these policies have raised concerns among policymakers and payers that dialysis facilities may be encouraging patients to maintain private insurance. This concern is borne out by dialysis facilities reporting a dramatic decline in the share of their patients who were covered by Medicare, from an average of 89% in 2005 to an average of 65% in 2016. In this study, which was led by our group, we were unable to determine the type of insurance coverage of the remaining 11% to 35% of patients, because the national registry for ESKD patients and providers only reports coverage of Medicare vs non-Medicare insurance.

In order to accurately assess trends in insurance coverage and payments, we will need detailed specification of type of insurance among patients not covered by Medicare. Potential alternative sources of coverage include commercial coverage through an employer, private individual insurance through an ACA exchange or off exchange, state Medicaid coverage and private Medicare Advantage. It is unclear whether the purported diversion of patients from Medicare to private insurance may adversely affect patient care and increase national spending (private and public) of ESKD.

This project will extend our prior on trends in Medicare enrollment by linking the standard USRDS and Medicare data with Medicaid and private insurance data in Colorado to precisely understand what is causing the trend we documented (Aim 1), who it affects (Aim 2), and what the implications are for payers and patients (Aim 3). In addition, these linkages will allow us to validate USRDS insurance coverage indicators for policy and research communities. We propose to use the Center for Improving Value in Health Care (CIVHC) data to identify patient-level insurance coverage information across Medicare, Medicaid, and private insurance. We will address three questions related to dialysis patients in Colorado:

1. Did rates of Medicare and private insurance coverage among new ESKD patients change after federal policies impacting ESKD care payment and coverage?
2. What patient (e.g., demographic, clinical) and regional characteristics are associated with transition to enrollment in Medicare during the 1st year of incident ESKD?
3. Is patient's health insurance program associated with greater likelihood of home dialysis (modality of treatment that is less costly to providers and payers) and overall payments for dialysis within one year of initiation?

This study will conduct novel linkages of national disease registry and CIVHC's comprehensive payer data (e.g., traditional Medicare, Medicare Advantage, and non-Medicare sources such as Medicaid and commercial payers) to identify the policy implications of this dramatic change in health insurance coverage among ESKD patients. Specifically, it will enable the most complete ascertainment of ESKD patient payers known to date. Results will inform the feasibility of larger-scale data linkages and will also constitute preliminary data for further study to comprehensively describe the types of patients disproportionately impacted by these changes and evaluate the consequences of federal reforms on payers and patients.

Of note, we will need exempt approval for this protocol prior to submitting and executing any Data Use Agreements. We will furnish the executable DUAs to the IRB through a protocol amendment as soon as they are completed.

Briefly describe research/project activities occurring at Duke, including the source of all data /samples:

- Do not copy and paste an external entity's summary. Please limit to 3 paragraphs.

Study Design: We will conduct a retrospective cohort study on a sample of patients with incident ESKD in 2013-2017 in Colorado, which allows us to observe payer trends over years of data available through CIVHC and the USRDS. Temporal shifts in insurance coverage would be most observable among incident patients because patients with newly diagnosed ESKD may enroll in Medicare and are unlikely to dis-enroll thereafter. Patients will be excluded if they are not residents of Colorado, have missing demographic information, had no record of dialysis modality type by day 90, or had missing or invalid zip codes for assignment to dialysis markets. We define markets as Dartmouth Atlas hospital service areas (HSA).

Data Sources: Data for this project will come from CIVHC and USRDS Standard Analytic Files. CIVHC contains longitudinal enrollment and claims history on patients in Medicare fee-for-service, Medicare Advantage, Medicaid, and commercial insurance (e.g., state exchange, individual, group coverage). It will therefore serve as the primary source of data for identifying patient insurance enrollment and spending for general medical services, dialysis care, and pharmacy (e.g., provider charges, insurer reimbursement, and patient payments). The USRDS files contain information on ESKD patients' insurance status (Medicare versus not), demographic and clinical characteristics. The primary source of USRDS Medicare and non-Medicare status information comes from the longitudinal payer history file (USRDS-PAYHIST file), which is based on the Medicare Enrollment Database. Self-reported patient insurance status (not reliable), demographic and physician-reported clinical characteristics assessed at dialysis initiation come from the CMS Medical Evidence Report (CMS Form 2728, USRDS-MEDEVID file), which ESKD facilities are required to complete for all patients who begin treatment at their facility. Dialysis treatment modality is identified in the longitudinal Treatment History (USRDS-RXHIST) files, which are based on a combination of Medicare claims and provider-reported data. A benefit of the study is the standardized, claims-based granularity that CIVHC data contains for our variables of interest (e.g., type of insurance coverage, payment, race /ethnicity, comorbid conditions) as compared to USRDS.

Data Linkage: Data from CIVHC will be linked to USRDS, with requisite approvals by the Duke University Institutional Review Board, CIVHC and the USRDS. The study PI confirmed the following procedures for authorized linkage of data for this proposed study: she will facilitate coordination between USRDS and CIVHC to match populations with ESKD across their respective de-identified data and generate a new crosswalk between USRDS-CIVHC (Appendix C). Specifically, the study team will specify cohort criteria for CIVHC to generate a finder file of potential patients that will be directly transferred to USRDS. USRDS will generate a crosswalk of unique USRDS and CIVHC identifiers to enable the study team's linkage of USRDS and CIVHC data. Based on our current examination of national trends in Medicare enrollment, there will be roughly 4500 Coloradans with incident ESKD in 2013-2017.

Measures: Our primary interest is patients' insurance status during the first year of dialysis initiation, which reflects Medicare enrollment and coverage rules for the Medicare ESKD program during the time period in which coverage transitions would typically occur. Medicare enrollment includes those enrolled in traditional Medicare fee-for-service as primary payer, Medicare Advantage, or status with Medicare as secondary payer or pending Medicare enrollment. Non-Medicare enrollment may include Medicaid and/or commercial coverage. The CIVHC data will allow us to specify non-Medicare insurance coverage with greater precision than is possible in USRDS data. For each patient, we will ascertain insurance status across the first year onset of ESKD (incidence). We will summarize insurance status at dialysis initiation (i. e., day 1) and at days 90, 180, and 365 after dialysis initiation.

Dialysis treatment modality is derived from the USRDS-RXHIST file and defined as a dichotomous indicator of any use of peritoneal dialysis (the most common home dialysis modality) vs. hemodialysis within the first 90 days of initiating dialysis. While we found in our prior work that nearly all (~95%) patients remained on the same modality initiated in the first 90 days for up to 2 years after ESKD onset, we will explore the extent of changes in modality for potential adjustment in analysis because modality changes may be financially driven. Dialysis payments will come from CIVHC data; we will assign payments to the insurer type that a patient has on that day and aggregated in terms of total spending over 90 days, 180 days, and 1-year after dialysis initiation. As in prior work conducted by members of this study team, we will also calculate payment per dialysis treatment day (e.g., including payments for the dialysis procedure, dialysis-related medication, and ancillary services). This approach will enable comparisons of daily treatment payments across various payment systems (e.g., Medicare prospective bundled payment and commercial fee for service). Payer and patient out-of-pocket spending will be examined in aggregate and separately, and adjusted for inflation (2017 dollars).

Analysis: We will conduct descriptive analysis of insurance status across time in the cohort of Colorado patients with incident ESKD overall to address Aim 1 and by subgroups (e.g., patients aged 18-64, and by race) to address Aim 2. To identify patient and regional characteristics associated with changes in insurance status over time, we will model Medicare enrollment as a time to event outcome and will use the cumulative incidence function at 1 year after dialysis initiation. Death and kidney transplant will be treated as a competing risk and we will censor data at 1) 1 year after dialysis initiation or 2) end of data availability (December 2017). A Cox model will be used on those patients not on Medicare at ESKD onset to assess the association between explanatory variables of interest: time (i.e., categorical year), insurance type at dialysis initiation, and insurance type interacted with year, adjusting for patient and regional characteristics. Generalized estimating equations will compare the likelihood of peritoneal dialysis use by insurance type. Insurer payment per dialysis treatment day will be compared by insurance type (Medicare, Medicaid, Medicare Advantage, other) to evaluate whether private insurers in Colorado pay more per session than traditional Medicare. To understand more aggregate costs, we will compare insurer payments and patient out-of-pocket payments by insurance type over 90 days, 180 days, and 1-year after dialysis initiation. For both unadjusted and adjusted analyses, we will use log-gamma mixed models (random intercept by person) with indicators for insurer type and adjusting for patient and regional characteristics.

Attach all documents such as questionnaires, surveys, scripts and/or agreements in the Initial Review Submission Packet.

Are you planning to consent subjects?

○ Yes ◉ No

Will PHI be accessed for ascertainment or recruitment?

○ Yes ◉ No

Will PHI be utilized without consent for the conduct of the research/project?

◉ Yes ○ No

Target Enrollment:

Number of consented subjects:

- Enter a single number. If you anticipate consenting a range of subjects, enter the upper limit of the range. The number should represent the maximum number of subjects for the life of the study.

0

Number of individuals whose data/samples will be used:

4500

Describe how research data will be stored and secured to ensure confidentiality:

The study investigators (V. Wang, C. Sloan) and statistical analysts (O. Osazuwa-Peters and L. Zepel) will have access to USRDS and CIVHC data. Study data are on password-protected servers maintained by Duke University. No data will be transferred to the hard drive of a desktop/laptop computer. We anticipate completion of this project within 1-2 years of receipt of the data from USRDS. This includes 12 months to clean and restructuring of data for data analysis, analytical modeling and specification, and final data analysis. The USRDS data will be destroyed at the end of the project. The CIVHC data will be destroyed at the end of the project.

In addition, the Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall.

Of note, we will need exempt approval for this protocol prior to submitting and executing any Data Use Agreements. We will furnish the executable DUAs to the IRB through a protocol amendment as soon as they are completed.

Describe how research data will be collected and/or transmitted during the research/project (ie, survey results entered by subjects, data transmitted to study team, data emailed to external sites).

Include information about the security of networks and any third parties that may be involved.

Study data are on password-protected servers maintained by Duke University. No data will be transferred to the hard drive of a desktop/laptop computer. The study investigators (V. Wang, C. Sloan) and statistical analyst (L. Zepel) will be the only study team members who will have access to the data in the password-protected servers maintained by Duke University. In addition, the Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall.

Request for Waiver or Alteration of Consent and/or HIPAA Authorization

Will the population include deceased individuals?

(•) Yes ( ) No

This waiver request applies to the following research activity or activities:

- [ ] Scheduling of research activities in MaestroCare and/or the recording of PHI via telephone for screening purposes prior to obtaining written consent for the research. Scheduling of research activities in MaestroCare and/or the recording of PHI via telephone for screening purposes prior to obtaining written consent for the research.
- [x] Ascertainment (identification, selection) and/or recruitment of potential subjects while recording identifiable private information, such as protected health information (PHI), prior to obtaining the subject's consent.
- [x] Conduct of the research project without obtaining verbal or written consent and authorization.

Note: Answer the questions below as they pertain solely to PHI collected prior to consent.

Provide the following information:

List the elements of informed consent and/or HIPAA authorization for which waiver or alteration is requested:

- Provide the rationale for each.

We request a waiver of consent and/or HIPAA authorization for the following elements:

- CIVHC data files: We request a wavier of consent and/or HIPAA authorization for use of the CIVHC data files. We will be executing a data use agreement (DUA) in advance of using the files and the files will be accessed in a secure, password-protected file system, so all identifiable information will be protected.
- USRDS data files: We request a wavier of consent and/or HIPAA authorization for use of the USRDS data files. We will be executing a data use agreement (DUA) in advance of using the files and the files will be accessed in a secure, password-protected file system, so all identifiable information will be protected.

List the specific protected health information (PHI) to be collected and its source(s):

- (Note: PHI = health information + identifiers)

We request a wavier of consent and/or HIPAA authorization for use of the CIVHC and USRDS data files. We will be executing data use agreements (DUA) in advance of using the files and the files will be accessed in a secure, password-protected file system, so all identifiable information will be protected. The CIVHC and USRDS data files will include a unique de-identified identification key that will allow us to link records between files.

In addition, of the 18 items considered to be protected health information (PHI), under the request for waiver or alteration of consent and/or HIPAA authorization, we will use the following from our patient sample:

Birth date
Age at ESRD onset
Gender
Race
Ethnicity
Dates of service / hospitalization
Death date
State
Zip code

Criteria for Waiver: The DUHS IRB may waive the requirement for informed consent and authorization if all of the following criteria are met:

- Please respond to each item in the space below using protocol-specific language to provide justification:

a) The research or clinical investigation involves no more than minimal risk to subjects:

The proposed work is a retrospective observational study of end-stage renal disease (ESRD) treatment in US patients – data for this study is secondary, administrative data – and therefore human subjects will not be directly involved in this research. Since no individual will be identified in the data analysis or results of the study, there are no known risks to patients or dialysis facilities in this study.

b) The waiver or alteration will not adversely affect the rights and welfare of the subjects. Include a description of any measures to be taken to ensure that the rights and welfare of subjects will be protected:

The waiver of consent and/or HIPAA authorization for access and use of the CIVHC and USRDS files will not adversely affect the rights and welfare of the subjects. The version of the CIVHC and USRDS files that Duke's Department of Population Health Sciences receives will only include indirect identifiers, making it difficult to identify specific individuals in the data.

We receive the CIVHC and USRDS data on a password-protected file system. Duke Health Technology Solutions (DHTS) manages the servers and networks where the electronic study data will be stored. DHTS has extensive electronic data safeguard procedures in place. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All access to files and directories are controlled by groups and user rights. All data are securely stored on servers that are behind the Duke firewall. Data will be stored and analyzed on DHTS encrypted servers.

All analysis of CIVHC and USRDS data will be performed within PACE. PACE is the Protected Analytics Computing Environment at Duke and it provides a full function, high capacity environment for analyzing data. It is a computation infrastructure behind the Duke Health firewall which is hosted by the Duke Data Centers and adheres to all of Duke's security protocols. PACE allows Duke researchers and external collaborators, where appropriate, to work together on projects using a common data warehouse. PHI is housed in an environment that meets best practice standards for data protection covering HIPAA, 21 CFR Part 11, and Federal Information Security Management Act (FISMA). Duke faculty, staff and collaborators' access to these data are managed and monitored by access control measures overseen by project leadership.

All data transactions within PACE can be monitored and audited. All computations can be run on the servers and no data can be removed from the serves and stored in other locations, except via an honest broker where the approved IRB protocol supports that transfer. Results from the analyses can be moved out of PACE, but must be reviewed by an honest broker to confirm that all PHI has been de-identified.

Of note, all data use agreements (DUA) will be fully executed and in place for the use of the CIVHC and USRDS data files. We will need exempt approval for this protocol prior to submitting and executing any Data Use Agreements. We will furnish the executable DUAs to the IRB through a protocol amendment as soon as they are completed.

c) Whenever appropriate, the subjects will be provided with additional pertinent information after participation:

Not applicable – retrospective analysis of administrative data.

d) If this research activity relates to research involving deception, explain how subjects will be provided with additional pertinent information after study participation and what information will be provided. Otherwise indicate "not applicable":

Not applicable – the proposed work is a retrospective observational study of ESRD treatment in US patients.

e) The use or disclosure of protected health information involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of the following elements (e1. and e2.)

Demonstrate that the use or disclosure of PHI involves no more than minimal risk to the privacy of subjects by describing the plans requested below:

e1) An adequate plan to protect the identifiers from improper use and disclosure. Describe the plan (how protection will be accomplished) and indicate where the PHI will be stored and who will have access:

Minimal risk to subjects and privacy protection: The datasets to be used for this study are administrative. With the exception of patient residence zip code, birth, death and treatment dates, personal identifiers will be removed or encrypted for analysis. The use of personal identifiers will be limited to 1) creating demographic measures of ESRD patients and 2) construct a longitudinal patient record that accounts for changes in patient demographics, insurance status, treatment modality, residence, or facility assignment for utilization and outcomes at the population level. To minimize the risk of personal identification of study subjects, retrospective data extracts conducted at the patient-level and maintained in working datasets that will not contain directly identifiable human subject data, once all linkages across datasets and years are completed. . To further minimize risk, patient-level data is de-identified (i.e., Social Security Number or CMS Beneficiary ID is not provided in the USRDS registry data). Last, investigators will not publish or disclose data or results that identify individual patients or providers, or from which such identities could be inferred.

Data storage and security*:* Study data will be handled and analyzed at Duke University by approved study team members. We will extract data from the USRDS and CIVHC files, abiding by terms set forth in the executable DUAs between Duke University and NIH-NIDDK /USRDS, and Duke University and CIVHC. Copies of the fully executed Data Use Agreement will be furnished before any data is transferred or accessed.

Electronic data will only be transferred to other password-protected storage spaces (i.e., university-based server space). Only the investigators and data programmers indicated in executable IRB-approved protocols and DUAs will have access to storage and work with this data. The Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password

security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall.

e2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law.

Describe the plan (how and when identifiers will be destroyed and by whom). If there is a health or research justification for retaining the identifiers or such retention is otherwise required by law, provide the reason to retain identifiers:

To protect the confidentiality of patients and providers examined in this study, the study personnel will abide by the terms set forth by the executable DUAs with NIH-NIDDK/USRDS and CIVHC. The risk of personal identification of study subjects by the research team is possible with the use of identifiers (e.g., zip code, birth and death dates) that are necessary for the proposed work. To minimize the risk of personal identification of study subjects, retrospective data extracts conducted at the patient level and maintained in working datasets that will not contain directly identifiable human subject data, once all linkages across datasets and years are completed. Furthermore, data extracts of patient-level data and final analysis will be conducted at the primary research site (Duke University). To further minimize risk, patient-level data is de-identified (i.e., Social Security Number of CMS Beneficiary ID is converted to a project-specific identifier) in the USRDS patient registry files. Last, investigators will not publish or disclose data or results that identify individual patients or providers, or from which such identities could be inferred. Results of patient and facility data will be reported in the aggregate.

e3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity except (i) as required by law, (ii) for authorized oversight of the research study, or (iii) for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule. By electronically signing this submission, the PI provides this written assurance:

The protected health information that will be collected under this waiver will not be reused or disclosed to any person or entity except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule.

f) The research could not practicably be conducted or carried out without the waiver or alteration:

- Explain why informed consent/authorization can not be obtained from subjects.

Data for this study comes from administrative processed forms and claims as they are available (roughly 2-years from real-time) and thus, constitutes retrospective data (analysis). Not all patients with end-stage renal disease between the study years are expected to be alive at the time this study is conducted and throughout the study period. Nor will all study subjects be deceased by the end of the study period. Patient mortality is 1) relatively high in the ESRD population (25% in the first year of dialysis initiation) and 2) a key sampling criteria/outcome in this study. Therefore, access to deceased and non-deceased ESRD patient data is necessary to conduct the proposed research. In addition, personal identifiers that would facilitate contact (e.g., mailing address, telephone numbers) have been removed from the data to be used for this study. Therefore, consent of study subjects is impracticable and the proposed research cannot be carried out without an approved waiver of consent.

g) The research could not practicably be conducted or carried out without access to and use of the protected health information:

Patient information will only be used to 1) creating measures of ESRD patients and 2) construct a longitudinal patient record that accounts for changes in patient demographics, insurance status, treatment modality, residence, or facility assignment for utilization and outcomes at the population level. And since no individual will be identified in our analysis or dissemination of study findings, the results of the study are expected to be benign to the personal rights and welfare of the study subjects.

h) For research using biospecimens or identifiable information, the research could not practicably be carried out without access to and use of the protected health information:

Patient information will only be used to 1) creating measures of ESRD patients and 2) construct a longitudinal patient record that accounts for changes in patient demographics, insurance status, treatment modality, residence, or facility assignment for utilization and outcomes at the population level. And since no individual will be identified in our analysis or dissemination of study findings, the results of the study are expected to be benign to the personal rights and welfare of the study subjects.

IRB Notification of Decedent Research

In accordance with 45CFR164.512(i)(1)(iii), the IRB must approve research involving decedent's private health information. In order for the IRB to make the determination, please respond to each item in the allotted space below, using protocol-specific language to provide justification.

Provide a brief, meaningful description of the protected health information for which use or access has been determined to be necessary:

We have requested a wavier of consent and/or HIPAA authorization for use of the CIVHC and USRDS data files, which will include deceased individuals. We will be executing data use agreements (DUA) in advance of using the files and the files will be accessed in a secure, password-protected file system, so all identifiable information will be protected. The CIVHC and USRDS data files will include a unique de-identified identification key that will allow us to link records between files.

In addition, of the 18 items considered to be protected health information (PHI), under the request for waiver or alteration of consent and/or HIPAA authorization, we will use the following from our patient sample, which will include deceased individuals:

Birth date
Age at ESRD onset
Gender
Race
Ethnicity
Dates of service / hospitalization
Death date
State
Zip code

Check each statement below to attest to your knowledge that:

- [x] The PHI to be used will be used solely for research.
- [x] All subjects to whom this form applies will be dead.
- [x] The PHI is necessary for the research.

- (•) You will not disclose such PHI (share with anyone from outside DUHS or the SOM/SON) without first removing all direct identifiers, and also all indirect identifiers including information about the patient's age if greater than 89 years (state instead that the age is 90+ years), any dates of health-related events, and any patient's address more specific than state or 3 digit zip code (thus the data become de-identified).
- ( ) Alternatively, you may choose to disclose this PHI, but, if so, you declare that you will maintain an accounting of this disclosure (commonly referred to as "tracking" the disclosure) for the patient's next of kin if requested.

Privacy and Confidentiality

Explain how you will ensure that the subject's privacy will be protected:

Consider privacy interests regarding time and place where subjects provide information, the nature of the information they provide, and the type of experience they will be asked to participate in during the research.

The proposed work is a retrospective observational study of ESRD treatment in US patients. The datasets to be used for this study are administrative. With the exception of patient residence zip code, birth, death and treatment dates, personal identifiers will be removed or encrypted for analysis. The use of personal identifiers will be limited to 1) creating demographic measures of ESRD patients and 2) construct a longitudinal patient record that accounts for changes in patient demographics, insurance status, treatment modality, residence, or facility assignment for utilization and outcomes at the population level. To minimize the risk of personal identification of study subjects, retrospective data extracts conducted at the patient-level and maintained in working datasets that will not contain directly identifiable human subject data, once all linkages across datasets and years are completed. To further minimize risk, patient-level data is de-identified (i.e., Social Security Number or CMS Beneficiary ID is not provided in the USRDS

registry data). Last, investigators will not publish or disclose data or results that identify individual patients or providers, or from which such identities could be inferred.

Describe how research data will be stored and secured to ensure confidentiality:

How will the research records and data be protected against inappropriate use or disclosure, or malicious or accidental loss or destruction? Records and data include, for example, informed consent documents, case report forms or study flow sheets, survey instruments, database or spreadsheets, screening logs or telephone eligibility sheets, web based information gathering tools, audio/video/photo recordings of subjects, labeled specimens, data about subjects, and subject identifiers such as social security number.

Study data will be handled and analyzed at Duke University by approved study team members. We will extract data from the USRDS and CIVHC files, abiding by terms set forth in the executable DUAs between Duke University and NIH-NIDDK /USRDS, and Duke University and CIVHC. Copies of the fully executed Data Use Agreement will be furnished before any data is transferred or accessed.

Electronic data will only be transferred to other password-protected storage spaces (i.e., university-based server space). Only the investigators and data programmers indicated in executable IRB-approved protocols and DUAs will have access to storage and work with this data. The Duke Health and Technology Solutions group (DHTS) has extensive electronic data safeguard procedures in place to protect data. All users are required to have strong passwords that meet or exceed the DUHS standards for password security. Access to data is based on a person's role and need to know. All file and directory access is controlled by groups and users rights. All work areas are secured with electronic key access. All data are securely stored on servers that are behind the Duke firewall.

Application Questions Complete

Please click Save & Continue to proceed to the Initial Submission Packet.

The Initial Submission Packet is a short form filled out after the protocol application has been completed. This is an area to attach protocol-related documents, consent forms, and review the application.

DUHS INSTITUTIONAL REVIEW BOARD KEY PERSONNEL CHANGE ACKNOWLEDGMENT

The DUHS IRB has reviewed and accepted this Key Personnel change.
Protocol ID: Pro00109690
Reference ID: Pro00109690-KSP-2.0
Protocol Title: Examining Medicare Reliance after Implementation of Medicare Payment Reform and the ACA Marketplace
Principal Investigator: Virginia Wang
Review Date: December 16, 2021

Current Key Personnel
Frascino, Nicole; Genova, Jessica; Hammill, Bradley; Maciejewski, Matthew; Sloan, Caroline; Stagner, Michael; Wang, Virginia; Zepel, Lindsay

DUHS Institutional Review Board
2424 Erwin Rd | Suite 405 | Durham, NC | 919.668.5111
Federalwide Assurance No: FWA 00009025