Non-State Entity Application: VHCURES Limited Use Health Care Claims Research Data Set

VERMONT
GREEN MOUNTAIN CARE BOARD
144 State Street
Montpelier, VT 05620
802-828- 2177
gmcboard.vermont.gov

Application

APPLICATION INSTRUCTIONS

Introduction

The Vermont Health Care Uniform Reporting and Evaluation System (VHCURES)

The Vermont legislature authorized the collection of eligibility and claims data for Vermont residents to enable the Green Mountain Care Board (GMCB) to carry out its statutory duties that include determining the capacity and distribution of existing resources; identifying health care needs and informing health care policy; evaluating the effectiveness of intervention programs on improving patient outcomes; comparing costs between various treatment settings and approaches; providing information to consumers and purchasers of health care; and improving the quality and affordability of patient health care and health care coverage. (18 V.S.A. § 9410)

The GMCB is required to make the VHCURES data and information available as a resource for individuals and entities to continuously review health care utilization, expenditures, and performance in Vermont to the extent permitted by the Health Information Portability and Accountability Act (HIPAA) and other pertinent state and federal laws.

The claims and eligibility data available under a data use agreement can be broadly grouped into three lines of business including commercial, Medicaid, and Medicare. The GMCB has independent discretion to make decisions regarding the use and disclosure of commercial insurer data. The Department of Vermont Health Access (DVHA) and the GMCB share discretion with respect to the Medicaid data subset. DVHA must approve the use and disclosure of Medicaid data and must sign the Data Use Agreement (DUA) for authorized users of the Medicaid data subset. Per an agreement with the federal Centers for Medicare and Medicaid Services (CMS), the Medicare data subset is available only to Vermont State Agencies and entities performing research that is directed and partially funded by the State of Vermont. Under a DUA between GMCB and CMS, GMCB has independent discretion to make decisions regarding the use and disclosure of the Medicare data subset by Vermont state agencies.

Vermont state agencies may apply for a standard comprehensive research data set that includes all unrestricted and restricted data elements for broad use internally and by state contractors. Non-state entities may apply for a DUA for a limited use health care claims research data set using a different application form. This type of data set excludes the Medicare data subset and is tailored to specific research purposes as approved by GMCB and DVHA if the Medicaid data subset is requested. Applicants who are non-state entities must justify requests for individual restricted data elements and explain how the requested restricted data elements are applicable to the intended research purpose.

Data Governance Council

The GMCB chartered the Data Governance Council (DGC) to oversee the stewardship of VHCURES including the development and revision of principles and policies to guide decisions on data use and disclosure. The DCG supports the GMCB decision-making process for applications requesting use and disclosure of VHCURES data sets by non-state entities as addressed in this application form.

Application Review Process

This application is required of non-state entities requesting a DUA for a VHCURES limited use health care claims research data set (hereafter referred to as a limited use research data set) with the option of including the commercial and Medicaid data subsets to support a project focused on a specific research purpose or study.

GMCB staff must deem this application complete before initiating the full review process. **This includes submission of all required and applicable optional attachments as listed in the Application Checklist in this application.** Applicants must include a full list of individuals who will have access to the data set upon the effective date of the DUA with this application. Applicants must file Individual User Affidavits (IUA) signed by the Authorized User (AU) or Principal Investigator (PI) for all data users listed on this application. AUs or PIs must ensure that IUAs are filed with GMCB for future data users prior to their access to the data set or risk forfeiture of the DUA and the data set.

After an application is deemed complete, GMCB will start the application review process that may include a public discussion of the application by the DGC. The GMCB has the discretion to approve or disapprove applications for a DUA. All requests for the Medicaid data subset must also be approved by the Department of Vermont Health Access (DVHA). The GMCB will provide DVHA with a copy of the complete application, following a review of the application by the GMCB. Applicants may also be required to obtain approval of the AHS Institutional Review Board (IRB) Committee. (See http://humanservices.vermont.gov/boards-committees/irb)

The Agency of Administration (AOA) under "Procurement and Contracting Procedures" of Bulletin 3.5 is required to review and approve the DUA after the GMCB and DVHA, if applicable, have approved the application for a DUA.

The GMCB must review and approve requests by non-state entities to redisclose data including custom extracts to contractors, subcontractors, or other external agents. Non-state entities must file data redisclosure request form(s) (DRRF) with the GMCB prior to redisclosing the data set or any extracts generated from the data set to any external agents. This ensures continued compliance with provisions of state and federal laws and regulations regarding the data. The GMCB must also review any proposal to change the use or research purpose of the data after the DUA has been issued for a specific research purpose. The GMCB may require the filing of a new application for a DUA after reviewing requests for change in data use under an existing DUA.

Final Steps in the Application Process

If approved by AOA, the GMCB and the applicant jointly enter into a DUA that is signed by the Authorized User, Principal Investigator, GMCB, and DVHA if the Medicaid data subset is included. Prior to receiving the data set approved under the DUA, all individuals accessing and using the data on behalf of the Authorized User must sign IUAs attesting to understanding the appropriate use and disclosure of the data set and agree to comply with the requirements. If GMCB declines an application, a written statement identifying the specific basis for denial of the application will be provided to the applicant. The applicant may resubmit or supplement the application to address GMCB's concerns including those of DVHA if Medicaid data are being requested. An adverse decision regarding an application may be appealed to the GMCB.

General Instructions

Applicants must complete all required sections of the application and submit an electronic copy of the completed application, including all attachments, to gmcb.data@vermont.gov. Incomplete applications will not be reviewed until the applicant has provided all required information. An application checklist is provided to help ensure that your application is complete. For questions about the application process, gmcb.data@vermont.gov

Definitions

Agent: Means any individual or entity (e.g., a contractor, subcontractor, grantee, or subgrantee) acting on behalf of the Authorized User and subject to the Authorized User's control or accessing the Data Set on behalf of the Authorized User.

Authorized User: The Authorized User (AU) is typically an organization or agency. The AU signatory to the Application and the DUA must have the authority to sign legally binding agreements on behalf of the organization or institution.

***Custom Extract*:** A custom extract includes the minimum necessary data to support the research purpose. A custom extract is a data subset or table generated from the commercial and Medicaid data subsets. The Medicare data subset is only available to Vermont state agencies under the data use agreement between CMS and the GMCB.

This process ensures continued compliance with the requirements of the DUA and particularly supports the concept of using the minimum necessary data to support the approved research purpose. For example, if the study approved under a VHCURES DUA addresses pediatric asthma in the Medicaid population, the GMCB may approve use of a custom extract that includes Medicaid paid claims data for enrollees under the age of 19 only.

Data Custodian: The data custodian is responsible for the establishment and maintenance of physical and technical safeguards to prevent unauthorized access to and use of the data set. Agencies may designate multiple data custodians for different departments and programs. The data custodian(s) typically coordinate the receipt of the approved data set from GMCB's data consolidation vendor. The principal investigator may also be the data custodian. State contractors or other agents approved by GMCB to receive the data set or custom extracts after a review of a Data Redisclosure Request Form must identify and file contact information for their data custodian(s) with the GMCB.

Data Redisclosure: Any Vermont state agency or non-state entity with a VHCURES DUA that intends to redisclose the VHCURES data set or any custom extracts of the data set to external agents to support projects approved under the DUA must file a Data Redisclosure Request Form (DRRF) with the GMCB for review and approval prior to the redisclosure.

After the GMCB has reviewed a DRRF and approved redisclosure of data to an external agent, the GMCB may request its data consolidation vendor to generate custom data extracts for external agents or permit the external agent to access the data enclave hosted by the vendor. Use of services provided by the GMCB's data consolidation vendor may require payment of a fee to the vendor.

Institutional Review Board (IRB): An institutional review board (IRB), also known as an independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), is a committee that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans.

Personally Identifiable Information (PII): The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. It is important to recognize that non-PII can become PII whenever additional information is made publicly available when combined with other available information.
Source: https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act

Principal Investigator (PI): The Principal Investigator means the individual designated by the Authorized User to be responsible for ensuring compliance with all the restrictions, limitations, and conditions of use and disclosure specified in the DUA. The Principal Investigator may delegate technical responsibility to other personnel for the establishment and maintenance of security arrangements to prevent unauthorized access to and use of the data.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

State Entity: Vermont state agencies, contractors, or other external agents performing work for the State of Vermont. A non-state entity is not a Vermont state agency or an agent performing work directed and funded by the State of Vermont.

Application Checklist **(For use by the applicant. Applicants must include all required attachments and applicable optional attachments)**

Completed Application

□ **Section 1:** Research Summary

□ **Section 2:** Data Management Plan

□ **Section 3:** Project Team (*Including data users for whom signed IUAs are being filed*)

□ **Section 4:** Data Procurement and Price

□ **Section 5:** Data Transmission and Receipt

□ **Section 6:** Signatures

Required Attachments

□ **Attachment 1:** Data Use Agreement template (*Will be signed by the Authorized User and Principal Investigator after the application is approved by Agency of Digital Services for Agency of Administration, GMCB, and DVHA (if Medicaid data is to be disclosed under the DUA*)

□ **Attachment 2:** Entity's Data Governance and Protection Policies and Procedures

□ **Attachment 3:** Limited Use Research File Specification (Includes justification for requesting restricted data elements as necessary to support the specific research purpose)

Optional Attachments Applicable to Proposed Redisclosures of the Data or Extracts

□ **Attachment 4:** Copy of proposed contracts, subcontracts, or any other agreements with external agents requiring redisclosure of the data set or custom extracts

□ **Attachment 5:** Data Redisclosure Request Form(s) (DRRF) must be filed for every external agent identified under Attachment 4 to whom the data or data extracts will be re-disclosed by the entity in possession of the DUA

□ **Attachment 6:** Data Governance Policies and Procedures for every external agent identified under Attachment 4 that will be receiving and managing the data set or extracts of the data set

Miscellaneous Optional Attachments

□ **Attachment 7:** If applicable to this application, Institutional Review Board approval document

□ **Attachment 8:** Other materials requested by the GMCB for the purpose of reviewing the application

APPLICATION

Section 1: Research Summary

Section 1 summarizes the specific research purpose of the project requiring access to a limited use health claims research data set during the term of the DUA. The Authorized User must discuss any proposed changes in the research purpose that are not specified in this application with the GMCB. The GMCB may require the filing of an application for proposed changes in data use and the research purpose.

Answer every question in this section. If a question does not apply to your research project, indicate that the item is "Not Applicable." Do not leave a question blank or the application will be deemed incomplete.

1-1. Project Overview

Authorized User Signatory Name & Title: **Kristina Lowell, Vice President of Health Care Evaluation Research**

Organization/Entity Name: **National Opinion Research Center (NORC)**

Type of Organization

□ Federal or State government entity outside of Vermont

□ Contractor of Federal or State government entity outside of Vermont

□ Academic Institution

X Non-profit research organization

□ Participant in the Vermont health care system financing, insurance, or delivery system with direct impacts on the Vermont population

□ Participant in health care financing, insurance or delivery systems outside of Vermont

□ Health care enterprise such as manufacturers or distributors of pharmaceuticals and medical technology; designers and developers of health systems and facilities, etc.

□ Other: Please describe below

Principal Investigator Name & Title (if different from Authorized User): **Sai Loganathan, Senior Research Scientist**

Project Name (Specify a topic or study): **Evaluation of the Vermont All-Payer ACO Model**

Brief Project Description (Summary of subsection 1-5-1):

The Vermont All-Payer ACO (VAPACO) model aims to improve statewide health care spending, population health outcomes, quality, and value by aligning payment structure and incentives across payers. The VAPACO model assumes that large-scale integration of population health initiatives will lead to statewide improvement in health outcomes and reductions in spending and utilization. Both Vermont and the Centers for Medicare & Medicaid Services (CMS) anticipate that the VAPACO model will encourage providers to make changes at the practice level; thus all beneficiaries (not just those enrolled in ACOs) will reap the benefits of more efficient care.

Our evaluation of the VAPACO model will answer questions about model impact on population health outcomes; statewide spending (Medicare, Medicaid, commercial, and all-payer); delivery system and process measures; other measures of healthcare utilization, spending, and quality of care; and implementation challenges and successes.

Project Start Date: **September 1, 2018**

Project End Date: **March 31, 2024**

Funding Source(s)

☐State ☒**Federal** ☐ If Other, please describe:

Line of Business data subset included in data request:

☒**Commercial** ☒**Medicaid (DVHA must approve Medicaid data use)**

If you intend to redisclose the data to contractors, subcontractors, or other external parties, identify parties (Must align with documents filed under Attachments 4, 5, and 6):

The NORC research team has no plans to redisclose data to any external party at this time.

1-2. Authorized User Acknowledgements

Please initial each item indicating your agreement with conditions of use.

KWAH) *I agree that I have the authority to sign legally binding agreements on behalf of the organization or institution as applicable to this application and the attached Data Use Agreement (DUA).*

KWHZ ( )	*I have read and agree to the terms of the attached DUA. I understand the contents of the attached DUA may only be modified or amended in writing upon mutual agreement of both parties.*
KWHZ ( )	*I have read and agree to cooperate with the GMCB to amend the DUA from time to time to the extent necessary for the GMCB to comply with changes to 18 V.S.A. § 9410, HIPAA, or other legal requirements that may apply to the Data Set.*
KWHZ ( )	*I understand and agree that I am required to file signed Individual User Affidavits (IUAs) with the GMCB for every individual data user within my organization and those employed by any contractors, subcontractors or organizations outside my organization approved by the GMCB to access and use the VHCURES data set. I must file the IUAs prior to receipt of the data set and as new users join the project or risk forfeiture of the data set and the DUA.*
KWHZ ( )	*I understand and agree that I must obtain the express written approval of the GMCB to release the data set or any derived extracts of the data to any agents or parties outside my organization. I must file a Project Review Form (PRF) with the GMCB for review prior to any re-disclosure of the data set to parties outside of my organization or risk forfeiture of the data, the DUA and be subject to civil and criminal sanctions and penalties for an unauthorized disclosure of data.*

1-3. Project Questions

Answer the following questions about your research project.

Yes ☐ No☒	Is the project directed by the State of Vermont including Vermont state agencies and UVM?
Yes ☐ No☒	Is this project partially or wholly funded by the State of Vermont?
Yes ☐ No☒	Will products generated from the project be used for a proprietary, commercial purpose to generate revenues and income? **If yes, explain below:**
Yes ☒ No☐	Is the project useful for determining the capacity and distribution of existing health care resources?
Yes ☒ No☐	Is the project useful for identifying health care needs and informing health care policy?
Yes ☒ No☐	Is the project useful for evaluating the effectiveness of intervention programs on improving patient outcomes?
Yes ☒ No☐	Is the project useful for comparing costs between various treatment settings and approaches?
Yes ☒ No☐	Is this project useful for providing information to consumers and purchasers of health care?
Yes ☒ No☐	Is this project useful for improving the quality and affordability of patient health care and health care coverage?
Yes ☐ No☒	Does the project directly support public health activities?
Yes ☐ No☒	Does this project support educational purposes such as exploring the claims data for quality, potential uses, health services research training, or integration with other data sets?
Yes ☒ No☐	Does this project propose to link VHCURES data with any other individual record-level data sets? *If yes, describe the data sets and proposed methodology for linking in Section 1-5-4.*
Yes ☐ No☒	Does this project anticipate re-disclosure of the data set, custom extracts or analytical files generated from the data set to any identifiable external agents under contracts, grants, and agreements for research purposes that have been specified? *If yes, file Attachment 4, 5, and 6.*

1-4. Requested Data

Indicate the data files requested in this application.

File Type	Commercial Insurers	Medicaid[1]	Medicare[2]	Data Years or Date Range[3]
Medical Eligibility-VT Residents	☒	☒	Not applicable	2011-2022
Medical Claims-VT Residents	☒	☒	Not applicable	2011-2022

Medical Eligibility- 5% National Sample	Not applicable	Not applicable	Not applicable	
Medical Claims- 5% National Sample	Not applicable	Not applicable	Not applicable	
Pharmacy Eligibility	☒	☒	Not applicable	**2011-2022**
Pharmacy Claims	☒	☒	Not applicable	**2011-2022**
Medicare Part D Event- VT Residents	Not applicable	Not applicable	Not applicable	
Medicare Part D Event- 5% National Sample	Not applicable	Not applicable	Not applicable	
Medicare MEDPAR	Not applicable	Not applicable	Not applicable	

[1] The Department of Vermont Health Access (DVHA) must approve uses and disclosure of Medicaid data.

[2] Medicare data may only be used for research directed and partially funded by the state of Vermont.

[3] VHCURES data are available on a consolidated CY quarterly or annual basis on paid claims date basis starting with CY 2007.

1-5. Project Overview

1-5-1. Summarize the purpose and objectives of the proposed research. Describe how the research will contribute to generalizable knowledge that would also be applicable to the Vermont population, health, and health care and, if applicable, to the State of Vermont supporting the development, implementation, and evaluation of programs administered by Vermont state agencies.

NORC's evaluation of the Vermont All-Payer ACO model will answer questions about how stakeholders at various levels implemented the model, and associated challenges and lessons learned; impact on population health outcomes; statewide spending (Medicare, Medicaid, commercial); delivery system and process measures; and other measures of health-care utilization, spending, and quality of care. This evaluation will also assess the motivations, perceptions, and implementation experience of participating providers. To fully understand the context in which the model is being implemented, the evaluation will capture changes in the characteristics of the markets, organizations, provider networks, and aligned ACO populations during the implementation period.

The analyses using VHCURES data will assess the model's impact on claims-based outcomes among the commercial and Medicaid populations. We will use quasi-experimental designs, such as synthetic control methods (SCM) and difference-in-differences analyses with group-specific trends, to assess the impact on health spending and utilization for these two populations, as well as ACO-aligned Vermonters within these two populations.

Results from this evaluation will be used to assess the success of this innovative model, providing Vermont, external stakeholders, and other interested states the ability to assess whether this type of delivery system reform is worth pursuing and/or expanding. As more states explore innovative ways to deliver health care to their populations, this evaluation will serve as a model to hold up Vermont's innovative methods and successes and will be an essential piece of evidence for the all-payer ACO model.

1-5-2. Summarize the credentials, skills, and experience of the Principal Investigator and key research staff that are evidence that the Data Set will be used to conduct and support systematic investigations guided by expertise in the subject matter and research methods, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Sai Loganathan, PhD, M.P.A. is a Senior Health Economist and full-time employee at NORC, has more than ten years of experience overseeing mixed-methods evaluations, overseeing data analysis tasks involving administrative and survey data, and serving as a subject matter expert on Medicare and long-term care policy. Loganathan previously served as quantitative evaluation lead for the Arizona Medicaid supportive service expansion evaluation for members with severe mental illnesses. He currently serves as the survey sampling and analysis lead for the CMS Next-Generation ACO model evaluation. He recently served as the analytic lead for an AHRQ-funded evaluation to assess interventions aimed at reducing pressure ulcer incidence in nursing homes. Additionally, he oversaw claims-based analytics for rapid-cycle evaluations of Health Care Innovation Awards funded by CMS. He serves as a subject matter expert on cutting-edge mixed-methods evaluation methods, such as qualitative comparative analysis. He is a recognized expert in long-term care policy and evaluation research, and will serve as the Principal Investigator for this project.

Shriram Parashuram, Ph.D., is a Senior Health Economist at NORC. Parashuram has served as the quantitative lead on ongoing evaluation projects, including authorship of study design sections, developing analytic plans, presentations to clients, and managing budget & personnel for quantitative deliverables. He has served as quantitative lead on projects including the Center for Medicare and Medicaid Innovation's Health Care Innovation Awards, Evaluating State Health Information Exchange (HIE) under HITECH Act, Building Analytic Capacity for Monitoring and Evaluating the Implementation of the Affordable Care Act (Subcontract to RAND for ASPE), and Supporting eValu8 for National Business Coalition on Health (NBCH). He has also supported senior management in advancing NORC's capability to secure and deliver multi-year high-throughput quantitative health policy evaluations for federal clients. Prior to joining NORC, Parashuram was a graduate researcher at the University of Minnesota's Division of Health Policy and Management, where he worked on several CMS and AHRQ projects - examining the effect of Medicare's Physician Quality Reporting System

(PQRS) on enrollee outcomes, designing approaches to measuring efficiency of care provided by Medicare physicians, studying costs associated with chronic conditions for dual eligibles, investigating effects of rebalancing long-term care systems through home & community based services, and conducting economic valuations of pharmaceutical policies. Parashuram will serve as a Senior Advisor on this project.

Devi K. Chelluri, M.S., is a Statistician II for NORC at the University of Chicago with experience in Medicare and Medicaid claims analysis. Her responsibilities include developing statistical programs to analyze large datasets and providing consulting to other researchers. Prior to joining NORC, Chelluri was a Statistician for AdvanceMed, an NCI company working on fraud, waste, and abuse management for Medicare Parts A and B and Medicaid professional, hospital, long-term care, and pharmacy data in both fee-for-service and MCO in ZPIC 5. This included reviewing the data in both fee-for-service and MCO for potential vulnerabilities, developing new methodologies to identify potential vulnerabilities, researching fields to ensure that the most appropriate statistical techniques and methods are utilized, and presenting data findings to Medicare, Medicaid, and Federal personnel at state meetings. Chelluri has a background in statistics with a B.S. in Statistics from the University of Pittsburgh and a M.S. in Biostatistics from the University of Michigan. She is a member of the American Statistical Association, is a member of the Committee on Applied Statisticians, and is an Accredited Graduate Statistician™. Chelluri will serve as a programmer on this project.

Mina Zheng, M.Sc., is a Statistician at NORC's Center for Excellence in Survey Research. Zheng has four years of professional experience conducting quantitative health services research. She has published original research on various aspects of cancer care using administrative data, including the SEER-Medicare database. She is currently working on evaluation of the Next Generation Accountable Care Organization model of care delivery, where she uses Medicare claims to determine patterns of care utilization among beneficiaries. Zheng holds two M.Sc. degrees from Georgetown University in health policy and biostatistics, respectively. Zheng will serve as a programmer on this project.

Erin Ewald, Sc.M., is a Research Scientist in NORC's Health Care Research Department. She provides quantitative evaluation and project management support on a variety of tasks such as managing and analyzing data, quarterly and annual report production, site visit and focus group management, and evaluation of hospital-reported outcome measures. Currently, she is co-leading quantitative data analysis and rapid-cycle report production for the Next Generation Accountable Care Organization evaluation as part of a large team. Additionally, Ewald is part of a small team that is identifying and characterizing transgender Medicare beneficiaries based on fee-for-service claims as part of a contract with the CMS Office of Minority Health; these results are being disseminated via CMS data briefs, conference presentations, and peer-reviewed publications. Prior to joining NORC, Ewald received her Master of Science in Epidemiology from the Johns Hopkins Bloomberg School of Public Health. Ewald will serve as a senior analyst on this project.

1-5-3. If your project requires the use of Medicaid data, is the research intended to support public health activities? If yes, explain the application of the project to public health. If no, you may be required to obtain approval to use the Medicaid data from the AHS IRB Review Committee in addition to DVHA. See Optional Attachment 6.

Yes, this research is intended to support public health activities. One of the main goals of Vermont's All-Payer model is to improve population health, and through this project and the use of VHCURES data, we will be able to assess the impact of this model on public health systems and population health outcomes (specifically in regards to the commercial and Medicaid populations using VHCURES data).

1-5-4. Explain how you will ensure that your organization and external agents performing state-directed research will have access to the minimum necessary data to support specified research purposes and projects.

Vermont commercial and Medicaid claims data will be extracted from VHCURES and moved to NORC secure servers, where they will be de-identified. The de-identified commercial claims extracts will be transferred to NORC servers through the SFTP, and analysis will take place on these secure servers.

NORC's computer and data security program is compliant with federal government regulations and will be adapted to the requirements of this project, as needed. We enforce physical security measures designed to ensure that access to confidential data are restricted only to those employees who possess the need, as well as the authorization, to view such information. Project materials are protected through a multi-tiered approach of access control and monitoring, data encryption during transmission, and continuous upgrade of plans and policies to align with the changing security environment. All electronic project files and programs are stored on secure servers, and access to this project's shared space, managed by NORC, is restricted to authorized team members with clearance to use specific data. Partitioned network storage is provided for each project to mitigate the potential for data loss due to accidents, computer equipment malfunction, or human error, as well as to administer appropriate access rights.

All remote access to internal NORC computing resources requires two-factor authentication and encrypted channels. All of NORC's laptop computers are provisioned with an automatic full disk encryption system to protect against loss of sensitive data. Finally, NORC secures data transfer via the Internet by means of FIPS 140-2 compliant VPN. Data at rest are encrypted by means of FIPS 140-2 compliant whole-disk encryption technology.

1-5-5. List and describe any identifiable record-level data files or other record-level data sources you are planning to use in conjunction with the requested VHCURES data. If the files will be linked, explain the methodology for linking the data; if applicable, which files include direct personal identifiers and list the personal identifiers included in the files; and how the identity of individuals and their PHI will be protected from unauthorized disclosures within and outside your agency or organization.

Depending on the usability of the Medicaid data in VHCURES and available elsewhere (i.e., on CMS' Chronic Conditions Warehouse), the NORC team will consider linking select program participation variables in the Medicaid data to other sources, such as T-MSIS Analytic Files, using the Medicaid identifier in VHCURES to analyze impact of Blueprint initiatives on the target population. If a direct match is not possible or has a low match rate, we will use a combination of other identifiers (e.g., birth date, location).

All NORC staff are thoroughly trained annually on institutional confidentiality protection procedures and, when appropriate, the requirements set forth in the Privacy Act of 1974 and Privacy Act Regulations; the Health Insurance Portability and Accountability Act (HIPAA); by the Council of American Survey Research Organizations (CASRO); American Association for Public Opinion Research (AAPOR); and Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Upon hiring, all NORC staff members are required to sign a legally binding document called the "Statement of Professional Ethics," which emphasizes NORC's commitment to confidentiality. The statement explains the importance of confidentiality obligations and the consequences for breaking confidentiality. Any breach of confidentiality will result in disciplinary actions, including termination, a fine, and/or prosecution. Before hiring, all employees are subject to a background security check.

1-5-6. Identify and briefly describe the funding source(s) for the proposed research including both internal and external sources that may be in the form of state and federal funding, grants, and other sources. Describe the relationship between the funding source(s) and your organization.

The funding for this project comes from the Centers for Medicare & Medicaid (CMS), contract number HHSM-500-2014-00035I. NORC is an independent contractor for CMS for this evaluation.

1-5-7. Explain whether any component of the project was review and approved by an Institutional Review Board (IRB). If yes, attach the IRB review and approval under Attachment 7 to this application.

Yes, this project was reviewed by NORC's IRB in January 2019 and was determined not to be human subjects research. See Attachment 7 for the IRB Certification document.

Section 2: Data Management Plan

Section 2 relates to the policies and procedures your organization will use to ensure the proper management of the VHCURES limited use research data set and custom extracts derived from the data set. The GMCB recognizes the applicability of best practices for information security and privacy used in the CMS Data Privacy Safeguard Program (DPSP)[1] to the review of VHCURES DUA applications. Respond to every question about your organization's and those of approved entities external to your organization policies and procedures to ensure technical and administrative safeguards over the data.

Please answer the questions in each section with references to any attached documents including relevant page and/or section numbers. **Do not simply cite a cross-reference to the policy and procedure documents included under Attachment 2 and 6 of this application in lieu of answering each question. If questions are not answered completely, the application will be deemed incomplete.**

Any Data Redisclosure Request Forms (PRF) filed with this application for external agents under Attachment 5 may cite cross-references to this application for the same items in Section 2 below. Instructions are included on the DRRFs.

[1] "Data Privacy Safeguard Program Information Security and Privacy Best Practices" listed under Additional Resources published on https://www.resdac.org/resconnect/articles/158

2-1. Physical Possession and Storage of Data Files

Include specific references to the Data Governance and Protection policies and procedures documents filed with this application under Attachments 2 and 6 in your responses to the items below. ***Do not simply cite a cross-reference to the policy and procedure documents in lieu of answering each question.***

2-1-1. Describe how your organization will maintain an accurate and timely inventory of the VHCURES limited use research data set including original files received and any derived files used within your organization or released to external agents under state contracts and agreements.

The data will be kept in a manner that complies with all applicable laws and regulations. These objectives establish procedures for our systematic retention, storage, access, retrieval, and destruction of data:

- **Retain data in a secure and confidential manner for the minimum amount of time required by applicable law, regulation, or contract.**
- **Destroy data in a regular and methodical manner according to procedures and retention measures.**

2-1-2. Describe how your organization will ensure and monitor the compliance of all members of research teams both in-house and those employed by approved external agents with privacy and security policies and procedures as described in the documentation filed under Attachments 2 and 6 to this application and as required by the DUA.

All NORC staff and partners are thoroughly trained annually on institutional confidentiality protection procedures and, when appropriate, the requirements set forth in the Privacy Act of 1974 and Privacy Act Regulations; the Health Insurance Portability and Accountability Act (HIPAA); by the Council of American Survey Research Organizations (CASRO); American Association for Public Opinion Research (AAPOR); and Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Upon hiring, all NORC staff members are required to sign a legally binding document called the "Statement of Professional Ethics," which emphasizes NORC's commitment to confidentiality. The statement explains the importance of confidentiality obligations and the consequences for breaking confidentiality. Any breach of confidentiality will result in disciplinary actions, including termination, a fine, and/or prosecution. Before hiring, all employees are subject to a background security check.

2-1-3. Describe the procedures your organization will take to track the status and roles of the research team and notify GMCB of any project staffing changes.

The Project Director, Kristina Lowell, will have the main responsibility of notifying GMCB of any project staffing changes. Specifically, we will notify GMCB if a staff member leaves the project and/or NORC and no longer has access to the data, and we will notify GMCB when a new staff member is brought onto the project who may require access to the data. We will not permit any new staff members to access data until GMCB has been informed. In addition, the staff must have completed all standard NORC background checks and trainings as described above.

2-1-4. Describe your organization's training programs that are used to educate staff on how to protect sensitive data with personally identifiable information, protected health information, and other sensitive financial, socioeconomic, and personal information.

As part of a company-wide training program, the DGB provides continuing education and resources on data governance and privacy policies. Annually, all non-interviewer staff complete an online course that describes NORC's policies around data sharing, data security, privacy policies in place to protect respondent data, and staff resources and obligations.

2-1-5. Describe the protocol that would be followed by your organization or that of approved external agents, if applicable, to report and mitigate a breach in the security of the data set. Who will be responsible for notifying the GMCB (and CMS as applicable to Medicare data available only to Vermont State Agencies and agents of the State) of any suspected incidents of a breach in the security of the VHCURES data?

PII disclosures are managed through a formal incident response process, detailed in the NORC Incident Response Plan in Attachment 2. Security Incidents are tracked in NORC's Footprints help desk ticketing system, and are managed in accordance with the NORC Incident Response Plan. Historical incident records are retained in the Footprints ticketing system, as well as on a secure file server, with access limited only to security personnel, but which may be made available to affected clients upon request. The project director (Kristina Lowell) will be responsible for notifying GMCB of any suspected incidents of a breach in the security of VHCURES data.

2-1-6. What actions will your organization and approved external entities take to physically secure the data files? This includes files in motion, or on servers, local workstations, and hard media.

NORC's computer and data security program is compliant with federal government regulations and will be adapted to the requirements of this project, as needed. We enforce physical security measures designed to ensure that access to confidential data are restricted only to those employees who possess the need, as well as the authorization, to view such information. Project materials are protected through a multi-tiered approach of access control and monitoring, data encryption during transmission, and

continuous upgrade of plans and policies to align with the changing security environment. All electronic project files and programs are stored on secure servers, and access to this project's shared space, managed by NORC, is restricted to authorized team members with clearance to use specific data. Partitioned network storage is provided for each project to mitigate the potential for data loss due to accidents, computer equipment malfunction, or human error, as well as to administer appropriate access rights.

All remote access to internal NORC computing resources requires two-factor authentication and encrypted channels. All of NORC's laptop computers are provisioned with an automatic full disk encryption system to protect against loss of sensitive data. Finally, NORC secures data transfer via the Internet by means of FIPS 140-2 compliant VPN. Data at rest are encrypted by means of FIPS 140-2 compliant whole-disk encryption technology.

2-1-7. Please explain if your organization intends to transmit, store, or transfer the data set or any derived files outside the continental United States.

NORC has no plans to transmit, store, or transfer the data set or any derived files outside of the continental United States.

2-2. Data Sharing, Electronic Transmission, Distribution

Include specific references to the Data Governance and Protection policies and procedures documents filed with this application under Attachments 2 and 6 in your responses to the items below. ***Do not simply cite a cross-reference to the policy documents in lieu of answering each question.***

2-2-1. Describe what your organization's policies and procedures will be for sharing, transmitting, and distributing the VHCURES data set and any derived files.

NORC information system components protect the confidentiality and integrity of information transmitted over the network through the use of built-in operating system and application protections as well as other physical and logical protections. See section IT-26 in Attachment 2 for complete documentation of NORC's organizational policies.

The Juniper SA4500 FIPS SSL VPN appliance that NORC uses for remote VPN access employs TLSv1 (Transport Layer Security) to protect transmission confidentiality and integrity. All Domain Name Service (DNS) traffic is internal to NORC and not exposed to the public facing networks. DNS is integrated with active directory and updates are secure and dynamic. The Juniper SA4500 FIPS appliance is configured to accept TLSv1 protocol connections. The appliance's configuration is set to require at least 128-bit encryption to establish a connection.

The NORC infrastructure is a switched network, which enhances the confidentiality and integrity of transmitted information. NORC uses fiber optic cable to connect infrastructure equipment between floors. All network and telecommunication equipment is housed in locked facilities. NORC uses the following methods to provide transmission confidentiality and integrity:

- **Checksums defined by the TCP and UDP networking protocols.**
- **Checksums provided by the IPv4 header.**
- **Cryptographic mechanisms as defined in Section 4.1 above and 4.3 below.**
- **Enforcement of SMB signing.**
- **Switches and transmission lines are physically secured.**
- **Operating system protection mechanisms against common spoofing and man-in-the-middle attacks.**

NORC must employ FIPS 140-2 compliant cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures defined in NORC Physical and Environmental SOPs. For instance, NORC protects digital back-up media by encrypting the media so if something happens to that media in transit to the off-site storage facility or at the facility, the data on the tapes or files cannot be exposed.

2-2-2. The GMCB's preferred method of transmission of the data files is through a secure File Transfer Protocol (SFTP) transmission. If you anticipate requesting encrypted hard media, please explain the reasons that SFTP is not an option.

NORC does not anticipate requesting encrypted hard media; SFTP transmission is our preferred method of transmission.

2-2-3. Would your organization and approved external agents be interested in accessing a hosted data enclave or a researchers' workbench environment eliminating the transmission of data files via SFTP or via encrypted hard media outside of the hosted enclave? If yes, would the interest hold if there are fees for this service? If not interested at all or cautious, please explain your concerns.

NORC would not be interested in accessing a hosted data enclave because, given the nature of the analytic tasks, we anticipate computational constraints and data integration challenges. Our teams have experience with the SFTP process and we already have infrastructure in place to support this type of transmission; thus, we see no value add of switching to a hosted environment if it is not necessary.

2-2-4. Describe your organization's methods and those of approved external agents for tracking, monitoring, and auditing access and use of sensitive data such as the VHCURES data set.

NORC has developed standard procedures for tracking, monitoring, and auditing access to use of sensitive data like VHCURES. See sections K2 and IT-38 of Attachment 2 for complete documentation of NORC's policies for this topic.

Access to NORC systems and project resources is limited to those users who need the access to perform their duties. Unauthorized access to NORC and project information is strictly prohibited. By connecting to NORC's network, users consent to NORC's use of both active and passive systems to assess the security of NORC's network and all devices connected to it.
At project inception, a review of project-specific security needs is conducted. In addition to NORC's standard processes and technologies, NORC's standard application security practices may be augmented to meet unique privacy or security issues for a particular project to ensure the security of data from collection to management to dissemination. Project specific security requirements may not jeopardize the accessibility, confidentiality, or integrity of any NORC data or computing environment. The project requirement cannot violate any NORC security policies or violate any local, state, or Federal laws or regulations.

NORC applications that manage NORC and project confidential data are protected against unauthorized access and restrict authorized access to the minimum necessary level. The use of anonymous or generic user IDs to provide general login access to NORC network services is prohibited. Once logged into a NORC application system, each user ID is allowed access only to well-defined, limited views of the data and the user interface screens that support the type of action the user is allowed to take. Data- access restrictions are accomplished through the use of unique case identifiers that allow the database to create a partition between response data and data that could be used to identify an individual. Without authorization, users may not use a password, access a file, or retrieve any stored communication that is not their own or has not been properly directed to them.

The Infrastructure Security and Systems Operations (ISO) Department monitors the IT network and systems for signs of intrusion and other security violations, using software that proactively searches for security holes and recommends fixes. This includes monitoring all operating system and application system vendors for security patches and applying those updates, as necessary. NORC has strict controls regarding server access and administration. The ISO Department performs periodic security surveys and checks of network systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment. In addition, NORC periodically engages third-parties to conduct network security audits. An audit may include comprehensive attempts at network penetration from undisclosed sources and a review of policies and procedures.

NORC employs an automated Event Log Management system (ELM), to gather, store, and analyze information system audit records. The ELM system, Cygilant's SecureVue, polls events from server systems at least every 5, 10, or 15 minutes and receives syslog messages from network devices as they

occur. In addition to system events stored in the ELM, NORC maintains a repository of directory and file service events using Varonis's DataAdvantage tool. NORC coordinates its security auditing functions with other NORC entities requiring audit-related information in order to enhance mutual support and to help guide the selection of auditable events. The NORC Server Team coordinates with the NORC Network and Database Teams to verify that their respective applications and databases meet the defined auditable event capabilities. NORC's list of events that are to be audited includes an excessive or unusual use of a privileged account (e.g., failed login, creation, deletion, modification, password reset).

2-2-5. Describe the policies and procedures and procedures your organization and approved external agents use to define data access privileges for individual users of the data, including the Principal Investigator, Data Custodian, analysts and researchers, administrative support, and IT support.

NORC employs the concept of Least Privilege on its networks, allowing only authorized access to users necessary to accomplish tasks in accordance with organizational missions and according to their job roles. See section IT-04 in Attachment 2 for the full documentation and implementation of this policy.

Users of IT System accounts or roles with access to security functions or information use non-privileged accounts of roles when accessing other IT Systems functions. All IT Engineering, Network Services, and Technical Support Services (TSS) staff have access to various security functions employed within hardware, software and firmware and only personnel with roles associated with those security functions are granted explicit access to correlating technologies. Information systems privileges are configured by group policies.

Access to project files (such as the VHCURES data) is only granted as needed at the minimal level needed, and must be approved by the system owner for each user and each system. Project Director Kristina Lowell and PI Sai Loganathan will work together to determine the list of authorized data users based on their project roles; only individuals who require access to the data for data management or analysis activities will be granted access to the data files.

2-2-6. Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).

NORC has a number of Access Enforcement mechanisms that control access between users and objects (e.g., VHCURES data) at both the system and application levels and grant approved authorizations for logical access to the system in accordance with applicable policy across the NORC IT infrastructure. See sections K2, K6, IT-02, IT-05, IT-07, IT-26, and IT-55 in Attachment 2 for complete documentation of these NORC organizational policies.

NORC information system enforces approved authorizations for logical access to the system in accordance with applicable policies. This includes the use of Role-Based Access Control (RBAC), as well as access enforcement mechanisms such as access control lists and/or matrices and encryption to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information systems and at the application level where applicable.

Users are responsible for exercising safeguards and precaution to protect their userid and passwords. All actions performed with a personal password are the responsibility of the user assigned the password. Employees should never reveal their password to anyone. The following passwords standards must be followed for all NORC passwords:

- **All password are assigned to individuals;**
- **All passwords should contain a minimum of 8 characters;**
- **All passwords should contain at least one numeric digit and one special character (Ex. !, @, #, $, %, &, *);**
- **All passwords must be changed at least every 90 days (60 days for privileged accounts);**
- **Passwords should not be recorded or posted in obvious places. If passwords must be recorded, they must not be easily accessible;**
- **Passwords should not contain 3 or more consecutive characters of the User ID;**
- **Passwords should never be sent through unencrypted Email; and**
- **Passwords should not be the same as any of the previous 24 passwords.**

System administrators implement automatic account lockout controls in accordance with applicable NORC and Federal standards. These controls are applied to all users that have access to NORC systems. Automated Lockout is a mechanism that addresses minimum requirements for preventing unauthorized access to information, systems, applications, and networks via unattended servers, laptops and workstations regardless of location or network location. Though NORC employs automated lockout and/or logoff mechanisms under other circumstances such as session inactivity, this procedure specifically relates to automated lockout mechanisms in response to unsuccessful login attempts. Locking screensavers are employed and in use on all computers and mobile devices. Screensavers shall be automatically activated by the computer's operating system during Account Lockout to obfuscate screen information. The period of inactivity is determined by Federal Regulations implemented through CIS standards, group policy settings. The default policy related to Automatic Session Lockouts is set by group policy and is as follows:

Account Lockout Threshold	3 attempts within 15 minutes
Account Lockout Duration	15 minutes
Reset Account Lockout Counter After	5 minutes

Account Lockout in response to Unsuccessful Login Attempts applies regardless of the whether the login occurs via a local or network connection. Thus, Account Lockout applies to both NORC systems with moderate risk as well as NORC systems in common areas.

The information system or specified application prevents unauthorized access to the system using session locks, either by initiation from the user of that system or by the system itself. NORC has configured a Domain-wide policy that forces users to have any workstation or server automatically switch to a screen saver and lock after 900 seconds (15 minutes) of inactivity. This policy is automatically applied to any user that is added to the domain. The session lock, when activated on a device with a display screen, will place a publically viewable pattern onto the display screen, obfuscating what was previously visible on the screen. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Session locks are not to be used as a substitute for logging out of the information system, such as when one leaves at the end of the workday.

NORC utilizes FIPS 140-2 encryption in the following instances to enforce access restrictions (list not all-inclusive):

- **WinMagic Hard Disk Encryption on Laptop Computers (for data at rest)**
- **Juniper SSL VPN (for remote access by NORC users to the internal NORC network)**
- **Secure File Transfers (for data in transit)**
- **eIQ SecureVue Log Management System (LMS)**

2-2-7. If approved external agents will have access to the data please describe how that organization's analysts will access the data file, e.g., VPN connection, travel to your organization, or house the data at other locations.

N/A – no external agents will have access to the data file.

2-2-8. If additional copies of the data will be housed in separate locations, list the locations and describe how the data will be transferred to these locations.

N/A – no additional copies of data will be housed in separate locations.

2-3. Data Reporting and Publication

2-3-1. Explain your process for reviewing publications prior to dissemination to ensure accurate and appropriate representation of your data sources, analytic methodology, results, caveats, and disclaimers. Describe how your publications will be reviewed to ensure compliance with requirements in the DUA addressing small n suppression, disclaimer of any GMCB endorsement of findings, and data source citation.

Our team has a rigorous series of quality checks for data, code, and output in place that are required before any results are reported to a client or publically. Code and output are peer-reviewed by team members with high level of expertise in data analysis and data management, and once those are cleared and entered into a draft report, a team that ensure accuracy across the data and how it is being presented in the report. The reported findings are cross-checked by mid-level and senior analysts, editors, subject matter experts, and the team's reporting lead before being finalized. In all reports wherein we present findings from the VHCURES data, we will comply with requirements for small n suppression, include a disclaimer of any GMCB endorsement of findings, and cite GMBC as the data steward/owner and VHCURES as the data source.

2-4. Completion of Research Tasks and Data Destruction

2-4-1. Describe how you will complete the Certificate of Data Destruction for the data set and derived files stored by your organization or by approved external agents and how the data will be deleted, destroyed or rendered unreadable by all parties with access to the files upon completion of the project.

Media sanitization (i.e., data destruction) is the responsibility of NORC's Infrastructure, Security, and Operations team. See section IT-104 of Attachment 2 for NORC's full policy for media sanitization.

NORC clears backup data from disk and tape using CommVault's Secure Data Erase feature, which permanently erases any selected data from backups. While this is a permanent data deletion solution, it must follow the data destruction steps that must be executed outside of the backups to eliminate a residual risk of CommVault backing up data that we intend to permanently delete.

- **The Secure Data Erase operation makes the data inaccessible for browsing and recovery - the data will remain on the media and take up space until it is aged off according to the retention rules set for the data. However, data will not be recoverable using any data recovery methods. If the backup job is already content indexed, the data being erased will be removed from the index.**
- **Using Secure Data Erase, you can erase data such as file system, system state, and office communications server (OCS) data. Once the data is erase, NORC IT can generate a Job Summary report that provides proof of the erased Data job.**

NORC clears all laptop and desktop hard disk drives leaving its control using DBAN software in accordance with Department of Defence (DoD) Level 1 5220.22-M (3 passes). Any hard drive where DBAN will not run or if the drive is mechanically inoperable must be destroyed by physical means.

2-4-2. Describe your organization's policies and procedures and those of external agents used to protect VHCURES data files when individual staff members of research teams terminate their participation in research projects (which may include staff exit interviews, return of passkeys, and immediate access termination for example).

In the event that a team member (either external or internal) is no longer participating in this project or no longer employed by NORC or an NORC partner, access to the protected folders which house the data on NORC servers will be immediately terminated. The project director (Kristina Lowell) will be responsible for notifying GMCB of the change in staffing.

2-4-3. Describe your organization's policies and procedures to ensure original or derived data files, including non-published aggregate reports, are not used following the completion of the project.

Upon completion of the project and/or DUA expiration date, NORC will comply with all destruction instructions outlined in the DUA. If data is to be destroyed, NORC will provide GMCB with a certificate of destruction per specific DUA requirements.

Section 3: Project Team

In Section 3-4, list the anticipated individual users within your organization and external agents such as contractors and subcontractors, and project roles. **Signed IUAs for individual users within your organization and those employed by external entities accessing the data must be filed prior to receipt of the VHCURES data set and on an ongoing basis as project staffing may change.**

3-1. Authorized User (Can legally bind the applicant's organization to agreements)

Please provide contact information for the Authorized User's signatory.

Name and Title of Signatory for the Authorized User

Kristina Lowell, Vice President of Health Care Evaluation Research

Organization Name

NORC at the University of Chicago

Street Address

4350 East-West Highway, 8th Floor

City **Bethesda**	State **MD**	Zip **20814**

Telephone **(301) 634-9488**	Email **lowell-kristina@norc.org**

3-2. Principal Investigator

Please provide contact information for the PI if different person than the AU.

☐Same as Authorized User Signatory

Name and Title of Principal Investigator 1

Sai Loganathan, Senior Research Scientist

Organization Name

NORC at the University of Chicago

Street Address

4350 East-West Highway, 8th Floor

City **Bethesda**	State **MD**	Zip **20814**

Telephone **(301) 634-9346**	Email **loganathan-sai@norc.org**

Name and Title of Principal Investigator 2

Organization Name

Street Address

City

State

Zip

Telephone

Email

3-3. Data Custodian(s)

Provide contact information for the data custodian for your organization and the data custodians for any external agents such as state contractors, subcontractors or other organizations that will storing the VHCURES data set or derived files.

Name and Title of Data Custodian

Charles Armstrong, Director, Information Technology

Organization

NORC at the University of Chicago

Street Address

4350 East-West Highway, 8th Floor

City

Bethesda

State

MD

Zip

20814

Telephone

(312) 759-2387

Email

armstrong-charles@norc.org

Name and Title of Data Custodian

Organization

Street Address

City

State

Zip

Telephone

Email

Name and Title of Data Custodian

Organization

Street Address

City | State | Zip

Telephone | Email

3-4. Individual Users

Identify all individuals within your organization and external agents who will be participating on this project. These individuals may be project managers, analysts, IT professionals, or any other person who may have access to row-level data or aggregate reports prior to the suppression of small n. You must attach a signed individual user affidavit for each of these individual users prior to the receipt of the data after the DUA is approved including any users not identified on this list when this application was submitted.

Name	Organization	Project Role or Title
Sai Loganathan	**NORC at the University of Chicago**	**Principal Investigator**
Shri Parashuram	**NORC at the University of Chicago**	**Senior Advisor**
Erin Ewald	**NORC at the University of Chicago**	**Senior Analyst**
Mina Zheng	**NORC at the University of Chicago**	**Senior Programmer**
Devi Chelluri	**NORC at the University of Chicago**	**Senior Programmer**
Karen Swietek	**NORC at the University of Chicago**	**Senior Analyst**
Kathryn Segal	**NORC at the University of Chicago**	**Junior Analyst**
Brittany Branand	**NORC at the University of Chicago**	**Project Manager**
Abby Rosenbaum	**NORC at the University of Chicago**	**Senior Analyst**
Rajakumar Sankula	**NORC at the University of Chicago**	**Senior Programmer**
Bridget Whaley	**NORC at the University of Chicago**	**Project Manager**

Section 4: Data Procurement and Price

The authorized user will receive the data from the GMCB's designated data processing vendor for a fee determined by the number of years of data and whether any complex customization is required. The authorized use may contact the vendor in advance to confirm the exact pricing that generally runs about $5,200 for an extract of paid claims data spanning five (5) years. Prices are subject to change.

In the future, the GMCB may be offering access to the data through a hosted data enclave. This would eliminate or be an additional option for accessing the data via electronic SFTP transmission of the record-level data. GMCB will notify the authorized user for the DUA when this service becomes available as an option and how it will work as to number of user seats and pricing.

There may be fees for custom extracts. Typically, custom extracts are generated to support the data stewardship principle of disclosing the minimum necessary data to support the research purpose. Data users may be authorized to access a secured data enclave hosted by the vendor. Use of services provided by the GMCB's data consolidation vendor may require payment of a fee to the vendor. Fees will be determined on a case-by-case basis. Onpoint Health Data will manage any invoicing for fees.

The GMCB's designated vendor for the VHCURES Limited Use Research Data Set is:

Onpoint Health Data

Mailing Address:
75 Washington Avenue, Suite 1E
Portland, ME 04101

Physical Address:
55 Washington Avenue
Portland, ME 04101

Main Phone: (207) 623-2555
www.onpointhealthdata.org

Section 5: Data Transmission and Receipt

Use of an electronic secure File Transfer Protocol (SFTP) is the preferred mode of release for approved data extracts. Onpoint Health Data, the GMCB's data consolidation and warehousing vendor will provide an "Electronic Data Transmission Readiness and Logistics Checklist" to assist you in determining whether you are able to receive the transmission.

Please identify your primary contact below for setting up the logistics for SFTP transmission of the approved data extract. The primary contact must either be the Authorized User or Principal Investigator or Data Custodian identified on the DUA or be designated by the AU or PI.

As noted under Section 4, the GMCB may offer access to the data via a hosted data enclave in the future. Authorized users will be notified when this service becomes available.

Primary Contact for Planning Data Transmission Logistics

Name: Sai Loganathan

Title/Role in the Project: Principal Investigator

If not AU, PI or DC, designated by: N/A

Email Address: loganathan-sai@norc.org

Phone Number: (301) 634-9346

Organization/Agency Affiliation: NORC at the University of Chicago

Street, City, ZIP Address:
4350 East-West Highway, 8th Floor
Bethesda, MD 20814

Section 6: Signatures

All statements made in this application are true, complete, and correct to the best of my knowledge.

Authorized User Name: **Kristina Lowell**

Signature:

Date:

Principal Investigator 1 Name (if different from Authorized User): **Sai Loganathan**

Signature:

Date: 2/19/2019

Principal Investigator 2 Name:

Signature:

Date:

GMCB Processing Section

For GMCB Use Only

Date Application Deemed Complete:

DVHA Application Approval Date:

GMCB Application Approval Date/GMCB Initials:

Date Applicant Notified of Approval:

Application Disapproval Date:

Date Applicant Notified of Disapproval/GMCB Initials

Summary of reasons for disapproval: