DATA USE AGREEMENT

DUA # 25534

(AGREEMENT FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS)

CMS agrees to provide the User with data that reside in a CMS Privacy Act System of Records as identified in this Agreement. In exchange, the User agrees to pay any applicable fees; the User agrees to use the data only for purposes that support the User's study, research or project referenced in this Agreement, which has been determined by CMS to provide assistance to CMS in monitoring, managing and improving the Medicare and Medicaid programs or the services provided to beneficiaries; and the User agrees to ensure the integrity, security, and confidentiality of the data by complying with the terms of this Agreement and applicable law, including the Privacy Act and the Health Insurance Portability and Accountability Act. In order to secure data that reside in a CMS Privacy Act System of Records; in order to ensure the integrity, security, and confidentiality of information maintained by the CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and State of Vermont Green Mountain Care Board *(Requestor)* enter into this agreement to comply with the following specific paragraphs.

1. This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (HHS), and State of Vermont Green Mountain Care Bo *(Requestor)*, hereinafter termed "User."

2. This Agreement addresses the conditions under which CMS will disclose and the User will obtain, use, reuse and disclose the CMS data file(s) specified in section 5 and/or any derivative file(s) that contain direct individual identifiers or elements that can be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the files specified in section 5 and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services or any of its components with respect to the data specified herein. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS point-of-contact or the CMS signatory to this Agreement shown in section 20.

3. The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

4. The User represents, and in furnishing the data file(s) specified in section 5 CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

Name of Study/Project
Integration of Medicare Data with Data Resources used by the State to Examine Health Care Access

CMS Contract No. *(If applicable)*

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, that have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 5 will be put.

The User agrees not to disclose, use or reuse the data covered by this agreement except as specified in an Attachment to this Agreement or except as CMS shall authorize in writing or as otherwise required by law, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement. The User affirms that the requested data is the minimum necessary to achieve the purposes stated in this section. The User agrees that, within the User organization and the organizations of its agents, access to the data covered by this Agreement shall be limited to the minimum amount of data and minimum number of individuals necessary to achieve the purpose stated in this section (i.e., individual's access to the data will be on a need-to-know basis).

5. The following CMS data file(s) is/are covered under this Agreement.

File	Years(s)	System of Record
State of VT Cohort		
MBSF: Base, Cost and Use, Chronic Conditions	2007-2011	
IP, OP, SNF, Hospice, HH, DME, Carrier	2007-2011	
MedPAR, Part D Event	2007-2011	
Crosswalk Files (Bene ID to HIC, SSN and Name)	2007-2011	
5% Files	2007-2011	
MBSF: Base, Cost and Use, Chronic Conditions	2007-2011	
IP, OP, SNF, Hospice, HH, DME, Carrier	2007-2011	
MedPAR, Part D Event	2007-2011	

6. The parties mutually agree that the aforesaid files(s) (and/or any derivative file(s)), including those files that directly identify individuals or that directly identify bidding firms and/or such firms' proprietary, confidential or specific bidding information, and those files that can be used in concert with other information to identify individuals, may be retained by the User until 1 Year, hereinafter known as the "Retention Date." The User agrees to notify CMS within 30 days of the completion of the purpose specified in section 4 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, the User agrees to destroy such data. The User agrees to destroy and send written certification of the destruction of the files to CMS within 30 days. The User agrees not to retain CMS files or any parts thereof, after the aforementioned file(s) are destroyed unless the appropriate Systems Manager or the person designated in section 20 of this Agreement grants written authorization. The User acknowledges that the date is not contingent upon action by CMS.

   The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon notice of termination by User, CMS will cease releasing data from the file(s) to the User under this Agreement and will notify the User to destroy such data file(s). Sections 3, 4, 6, 8, 9, 10, 11, 13, 14 and 15 shall survive termination of this Agreement.

7. The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems **(http://www.whitehouse.gov/omb/circulars/a130/a130.html)** as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" **(http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf);** and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" **(http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf)**. The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from the file(s) specified in section 5 is prohibited. Further, the User agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in section 17 without written approval from CMS unless such movement, transmission or disclosure is required by a law.

8. The User agrees to grant access to the data to the authorized representatives of CMS or DHHS Office of the Inspector General at the site indicated in section 17 for the purpose of inspecting to confirm compliance with the terms of this agreement.

9. The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in section 5, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death.

   The User agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 5 or any data derived from such files) must adhere to CMS' current cell size suppression policy. **This policy stipulates that no cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed.** Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less. By signing this Agreement you hereby agree to abide by these rules and, therefore, will not be required to submit any written documents for CMS review. If you are unsure if you meet the above criteria, you may submit your written products for CMS review. CMS agrees to make a determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries.

10. The User agrees that, absent express written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement to do so, the User shall not attempt to link records included in the file(s) specified in section 5 to any other individually identifiable source of information. This includes attempts to link the data to other CMS data file(s). A protocol that includes the linkage of specific files that has been approved in accordance with section 4 constitutes express authorization from CMS to link files as described in the protocol.

11. The User understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from the appropriate System Manager or the person designated in section 20 of this Agreement.

12. The parties mutually agree that the following specified Attachments are part of this Agreement:

    Attachment A: DUA Attachment for State Request Opting In

13. The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement or another written authorization from the appropriate System Manager or the person designated in section 20 of this Agreement, CMS, at its sole discretion, may require the User to: (a) promptly investigate and report to CMS the User's determinations regarding any alleged or actual unauthorized use, reuse or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by CMS, submit a formal response to an allegation of unauthorized use, reuse or disclosure; (d) if requested by CMS, submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and (e) if requested by CMS, return data files to CMS or destroy the data files it received from CMS under this agreement. The User understands that as a result of CMS's determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

    The User agrees to report any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2580 or by e-mail notification at **cms_it_service_desk@cms.hhs.gov** within one hour and to cooperate fully in the federal security incident process. While CMS retains all ownership rights to the data file(s), as outlined above, the User shall bear the cost and liability for any breaches of PII from the data file(s) while they are entrusted to the User. Furthermore, if CMS determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the User agrees to carry out these remedies without cost to CMS.

14. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not exceeding $10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated sec. (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.

15. By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.

16. On behalf of the User the undersigned individual hereby attests that he or she is authorized to legally bind the User to the terms this Agreement and agrees to all the terms specified herein.

Name and Title of User *(typed or printed)* Dian Kahn, Director of Analysis and Data Management		
Company/Organization State of Vermont Green Mountain Care Board		
Street Address 89 Main Street		
City Montpelier	State VT	ZIP Code 05620-3101
Office Telephone *(Include Area Code)* 802-828-2906	E-Mail Address *(If applicable)* dian.kahn@state.vt.us	
Signature Dian KAHN		Date 4/1/2013

17. The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and will be the person responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

    The Custodian hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this Agreement on behalf of the User.

Name of Custodian *(typed or printed)* James H Harrison, President, CEO		
Company/Organization Onpoint Health Data		
Street Address 16 Association Drive		
City Manchester	State ME	ZIP Code 04351
Office Telephone *(Include Area Code)* 207-430-0682	E-Mail Address *(If applicable)* jharrison@onpointhealthdata.org	
Signature		Date 7/3/13

18. The disclosure provision(s) that allows the discretionary release of CMS data for the purpose(s) stated in section 4 follow(s). (To be completed by CMS staff.) PA03-RES

19. On behalf of _____ the undersigned individual hereby acknowledges that the aforesaid Federal agency sponsors or otherwise supports the User's request for and use of CMS data, agrees to support CMS in ensuring that the User maintains and uses CMS's data in accordance with the terms of this Agreement, and agrees further to make no statement to the User concerning the interpretation of the terms of this Agreement and to refer all questions of such interpretation or compliance with the terms of this Agreement to the CMS official named in section 20 (or to his or her successor).

Typed or Printed Name	Title of Federal Representative
Signature	Date
Office Telephone *(Include Area Code)*	E-Mail Address *(If applicable)*

20. The parties mutually agree that the following named individual will be designated as point-of-contact for the Agreement on behalf of CMS.

On behalf of CMS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name of CMS Representative *(typed or printed)* Cheryl Sample		
Title/Component Health Insurance Specialist, Division of Privacy Operations & Compliance, PPG, OESS, OEM		
Street Address 7500 Security Boulevard		Mail Stop N1-04-28
City Baltimore	State MD	ZIP Code 21244
Office Telephone *(Include Area Code)* 410-786-7185	E-Mail Address *(If applicable)* cheryl.sample@cms.hhs.gov	
A. Signature of CMS Representative Cheryl Sample		Date 7/25/13
B. Concur/Nonconcur — Signature of CMS System Manager or Business Owner Andrew Shetto/(CMS) CMS Privacy Board Chair		Date 5/28/13
Concur/Nonconcur — Signature of CMS System Manager or Business Owner Part D Cynthia Tudor/(CMS)		Date 7/19/2013
Concur/Nonconcur — Signature of CMS System Manager or Business Owner		Date

Attachment A

This Attachment supplements the Data Use Agreement (DUA) between the Centers for Medicare and Medicaid Services (CMS) and the State User. To the extent that this Attachment is inconsistent with any terms in the DUA, this Attachment modifies and overrides the DUA.

A-1. Use and Reuse of the Data: The User may use or reuse original or derivative data without prior written authorization from CMS for additional research projects if such research projects are: 1) directed and partially funded by the state and 2) would allow for a Privacy Board or an IRB to make the findings listed at 45 CFR 164.512(i)(2)(ii) if the anticipated data recipient were to apply for the data from CMS directly. In doing so, the User may disseminate original or derived information from the file(s) specified in Section 5 of the DUA, with or without direct beneficiary or physician identifiers, to other agencies of the User's State for research projects, including to any entity performing research that is directed and partially funded by the state.

A-2. Data Linking: As long as the resulting files are only used for research projects as described above in A-1, nothing in the DUA, including, but not limited to Section 10, prohibits the User from linking records included in the file(s) specified in Section 5 of the DUA to other sources of individually identifiable information.

A-3. Data Storage: The User may physically move, transmit, or disclose the file(s) specified in Section 5 of the DUA away from the site specified in Section 17 of the DUA provided that such action is limited to the disclosures described above in A-1 The User agrees to ensure that each data storage site includes the appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent the unauthorized use or access to the data, as is specified in Section 7 of the DUA. The User also agrees to keep a record of all sites where the file(s) specified in Section 5 of the DUA or any derivative data are stored.

A-4. Disclosure of Findings: The User agrees not to disclose, with or without direct physician identifiers, direct findings, listings, or information derived from the file(s) specified in Section 5 of the DUA, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce a physician's total Medicare reimbursements.

A-5. Security of the Data: The User agrees to contractually bind all recipients of protected health information from the file(s) specified in Section 5 of the DUA to the terms of the DUA related to use, re-use, and re-disclosure of the data, including, but not limited to Section 13. The contract must require all recipients of protected health information to: 1) immediately report any breach of personally identifiable information to the User; 2) return or destroy the data in the event the agreement with the User is terminated unless CMS determines the data may be retained; 3) take corrective actions for minor violations; and 4) return or destroy the data for major violations. The User agrees to report all violations to CMS and to abide by CMS' findings as to whether the violation is minor or major. The User also agrees to no longer release data to any individual or entity with a major violation.

A-6. Termination of the Agreement: In the event the Agreement is: 1) not renewed prior to the Retention Date specified in Section 6 of the DUA or 2) terminated for any reason, the User agrees to destroy the file(s) specified in Section 5 of the DUA or any derivative data at all sites where the User has physically moved, transmitted, or disclosed the file(s) to conduct additional research as described in A-1.

Upon termination of the DUA, the User must also complete certificate of destruction to cover all sites where the file(s) specified in Section 5 of the DUA were physically moved, transmitted, or disclosed.

A-7. Signature Addendum: No signature addendum will be required as a part of this DUA, instead, as specified in A-5, the User will contractually bind all recipients of protected health information to the terms of the DUA related to use, re-use, and re-disclosure of the data.

A-8. Additional Requirements: The User agrees to provide CMS with a quarterly report detailing to whom the data has been disclosed and for what they are using it, as well as any sites where the data has been physically moved, transmitted, or disclosed. At the request of CMS, the User agrees to notify CMS of a proposed re-disclosure of the file(s) specified in Section 5 of the DUA or any derivative data and allow a 30 day period for CMS to review and, if necessary, veto the data request.

Andrew Slutsky

For: Centers for Medicare & Medicaid Services

Dian Gatti

For: State Agency

For ResDAC and CMS Use Only

Date Reviewed by CMS Privacy Board:

Notes / Comments:

Privacy Board's Decision: Approved 5/28/13 Part D Approved 7/19/13

Signature of Board Member: Andrew Shubb/(as) Cynthia Tudor/(as)

Did the requestor demonstrate:

- Potential benefit to benes or the CMS Programs?
- Need for identifiable data?
- Impossible/impracticable to obtain patient consent?
- Minimal risk to benes' privacy if data are disclosed?
- Need to contact beneficiaries via Beneficiary Notification Letter?

Executive Summary | Data Management Plan | Log of Users | Dissemination and Reporting of Findings

Requesting State Agency (see Item 1 of DUA)	State of Vermont Green Mountain Care Board
DUA User name and title (see Item 16 of DUA)	Dian Kahn, Director of Analysis and Data Management
Study/Project Title	Integration of Medicare Data with Data Resources Used by the State To Examine Health Care Access, Utilization, Expenditures, and System Performance for the Vermont Population

CMS Research Identifiable Files (RIF) and years requested:

a. **Please list the CMS data files and years being requested *at this time*** (if requesting reuse of data, include DUA#(s) to be reused)(files and years listed here should match Item 5 of DUA):

Cohort for State of Vermont 100% beneficiary files
5% national sample files for benchmarking

Enrollment 2007-2011
Institutional & Non-institutional claims (Inpatient, Outpatient, SNF, Hospice, Home Health) 2007-2011
Carrier 2007-2011
DMERC 2007-2011
MedPAR 2007-2011
Part D event data 2007-2010
Crosswalk files that would allow the State to link to other State data 2007-2011

b. **If this study will require further years of CMS data that are not yet available for request, please list those CMS data files and years that will be required** (Note: Approval of data files for years that are not yet available will NOT be granted at this time, the information included here will simply provide CMS with an overview of your study):
The State of Vermont will need ongoing access to most current year for the files as listed above for statutorily mandated study of trends in health care access, utilization, expenditures, and program and system performance including the 2012 updates for Enrollment, Crosswalks and 2011 for Part D event data.

The base year for the Vermont All Payer Claims Database is 2007. Claims data for commercially insured and Medicaid populations has been consolidated through CY 2012 and 2013 data are being processed on monthly basis. The State of Vermont is interested in having an all-payer data set that is as timely as possible with adequate run-off periods for final action on payment fields.

Please list any non-identifiable or non-CMS files you are planning to use in conjunction with the above files for your analysis. (e.g. Provider of Services (POS) file, AMA Physician Masterfile, etc.)
Vermont Healthcare Claims Uniform Reporting & Evaluation System (state-mandated All Payer Claims Database), The Vermont Uniform Hospital Discharge Data Set, provider of service registries and rosters from state programs for payment reform and the health insurance and information exchanges.

EXECUTIVE SUMMARY

Please describe the research activities you plan to undertake with the Medicare files in 500 words or less. If you are requesting Part D data, briefly describe how the study will be enhanced with Part D data.

Vermont's Act 48 established an explicit state policy and infrastructure to contain costs and to provide, as a public good, comprehensive, affordable, high quality, publicly financed health care coverage for all Vermont residents. The four goals include reducing health care cost growth; ensuring access to and coverage for high-quality care; supporting population health improvement; and ensuring greater fairness in financing care. Decision makers need accessible, accurate and timely information to evaluate progress. The State needs robust capacity to convert diverse data into meaningful information.

Under the State Innovations Models (SIM) grant, Vermont is pursuing activities to implement three innovative provider payment models to encourage better coordination of care across providers, improve quality and attain better cost-management. The grant will support investments in "system infrastructure" including improved analytics and predictive modeling for monitoring system costs and quality and capacity to measure provider workforce needs.

Vermont has a state-mandated all-payer claims database (APCD) called the Vermont Healthcare Claims Uniform Reporting and Evaluation System (VHCURES). Prior to VHCURES, the State relied heavily on hospital discharge data for health care analytics that excluded other important categories of providers/services such as physician services and drugs. Limited data have been available for measuring broad and more granular trends in utilization and spending by payer and provider categories.

In addition to data for commercial medical health benefit plans, Medicare Part C, and Medicare Part D, the state Medicaid program has been filing monthly eligibility and claims data. The VHCURES data set starts with January 2007 and moves forward on a quarterly basis with monthly filings by commercial insurers and Medicaid. Since 16 percent of Vermonters are enrolled in Medicare, inclusion of Medicare claims data in VHCURES to measure, monitor, and evaluate population-based trends in access, cost, health, and quality of care is crucial for measuring impacts of provider payment models and other health care reforms.

In addition to the enrollment, claims files, and MedPAR, the Part D event data will be used in combination with the VHCURES Part D data that does not include all participating PDPs and Vermont beneficiaries. VHCURES includes pharmacy eligibility and claims data submitted by PDPs with minimum Vermont enrollment of 200 Vermont residents starting with a base data year of 2007 and moves continuously forward. PDE data will be used in a to enhance the available information on spending, utilization, prescribing patterns, access to pharmaceutical services, and care management studies in the aggregate and for specified diseases and conditions. Spending on drugs and supplies is the third largest category in health spending in Vermont following spending on hospital and physician services. It is a crucial

sector of service that needs to be included in analysis, modeling and forecasting health care spending, use, and patterns of care.

The crosswalk files will enhance linkage with other State data such as Medicaid for evaluation of access, cost, efficiencies, and coordination and quality of care for dually eligible individuals. The VHCURES claims data are de-identified but include unique person identifiers and data elements that can support probabilistic linkage across data sets supporting development of de-identified person-level records.

You are requesting Research Identifiable Files (RIF). Why can't Limited Data Set (LDS) files be used for this study?
This study requires access to individually identifiable data for the purpose of supporting linkage of beneficiaries with pre-Medicare payer data and other identified and de-identified data sources that would be needed to construct de-identified person-level records to track health/disease status, vital statistics, health care utilization and spending, and other metrics in an unduplicated manner on a longitudinal basis for Vermont residents. It is also important to identify full dates of service and other more granular information at the individual beneficiary level to support linkage for the purpose of de-identified reporting and analytics.

Is it feasible to obtain individual level authorization from Medicare/Medicaid beneficiaries for your research? Explain.
It is not feasible to obtain individual level authorization due to the high volume of subjects and longitudinal nature of the study that includes retrospective analysis for beneficiaries who may be deceased or no longer residents of Vermont.

How have you ensured that your data request includes the minimum amount of data necessary to achieve your research objectives? (Note here if you are a HIPAA covered entity)
The Green Mountain Care Board (GMCB) is not a HIPAA covered entity but adheres to HIPAA standards for protection of Personal Health Information under the provisions of the state mandate to collect and manage health data and state regulations pertaining to this activity. This request for data is the minimum amount required to meet the State's broad needs for analytics for the Vermont population.

If you intend on requesting the National Death Index segment of the Master Beneficiary Summary File, please complete the NDI Supplement.
__YES, I've included the NDI Supplement X NO, I'm not requesting the NDI

Is the research funded by a commercial entity, such as a pharmaceutical company?
__YES, research funded by a commercial entity X NO, research not funded by a commercial entity

> **If YES, the researcher attests that the commercial entity will not receive any individual data and that the researcher would have full editorial control over any publication regardless of the study findings.**
> __YES

DATA MANAGEMENT PLAN

Please reference the Data Management Plan Guidelines, Data Management Plan Evaluation Guide, and/or the FAQ document for more information on completing this section. This is found under the Executive Summary section of the New Study Requesting Data page.

1. **PHYSICAL POSSESSION AND STORAGE OF CMS DATA FILES**

1.1. Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).
Data Custodian – James Harrison, President & CEO
Network Administrator – Randy Nethers
Director of Information Services – Peter Burnell
Manager of Health Data Services – Gloria McCann

1.2. Explain the infrastructure (facilities, hardware, software, other) that will secure the CMS data files.

Technologies (Hardware/Software):
Network — Cisco 3750 core switches,
Cisco 2960 peripheral switches,
Cisco ASA 5510 firewalls,
Cisco 1841 routers
Data storage — Network Appliance FAS-3240 (All flat files and Oracle database files)
Sun (Oracle) Storagetek 6140 (storage for desktop VDIs),
Dell PowerVault NX3100 (archival),
Dell PowerVault T4000/2x LTO4 drives (tape back-up)
Storage area network (SAN) — Brocade Silkworm 300

Database — Oracle (11.2)
ETL – Pervasive Data Integrator(10.2.5) (Software Tool that moves/transforms claims data from flat files into Oracle database tables)
Java – Java SE 6 (Sun/Oracle Java Software platform) with Java Security and Cryptographic operations embedded

Onpoint contracts with Time Warner Cable (TWC) to provide co-location and network services in Portland, Maine. Onpoint maintains all critical production systems in the TWC facility but also maintains an in-house data center for noncritical services in Manchester, Maine. The Time Warner facility and network share the following features:

- 24-hour access via key code and swipe card
- 24-hour surveillance provided by Local Network Operations Center
- Elimination of third-party loop providers with the local loop owned and maintained by TWC

Onpoint's secure software systems are maintained by our systems administration staff.
All credentialed users, are provided with logins and passwords, which must be entered to gain access to all of our systems. Network access for user authentication is done by using Microsoft Active Directory, along with group policies which limit access to Files Shares and Systems.

To meet HIPAA's privacy restrictions, Onpoint's data collection system ensures that direct member identifiers remain safe through the use of a Triple DES two-way encryption algorithm. Using Onpoint's system, all direct member identifiers are encrypted as soon as they are uploaded to our secure systems.

All Onpoint hardware and networks are maintained by our professional team of System and Network Administrators, with primary and secondary physical firewalls in our Data Center.

As part of Onpoint's Information Security Program, both policy and procedures are stated that place PHI protection as the highest priority designed to meet or exceed:

- The Health Insurance Portability and Accountability Act (HIPAA).

- Breach notification as required by section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act
- The Payment Card Industry Data Security Standard (PCI-DSS) requirements
- Applicable security breach notification laws

Companion programs, plans, and standards (referenced below) are integral to the success of the information security program and are listed below:

- Security Awareness Training Program
- Incident Response Plan
- Disaster Recovery/Business Continuity Plan Procedures

Physical Safeguards – Onpoint's Data Center and Offices

- All Changes to Production Systems are documented and part of our overall Change Management Policies. These changes include hardware, software and user access.
- Disposal of any storage devices include rendering the device inoperable for use, which would include destruction of physical media.
- Access to the Data Center is tightly controlled.
- Access to Offices is limited to employees and guests with a formal sign-in access process.
- Access to hardware and software is limited to properly authorized individuals.
- Workstations are not allowed to store any Person level data. All Onpoint desktops run in our Data Center as Virtual Desktops(VDI), which enables Onpoint to control all access to data to software running in the Data Center.

Using guidance from NIST, including but not limited to security standards (800-53), risk management (800-30 & 37), and governance/policy (800-12), Onpoint has developed and maintains a robust Information Security Program. The organization is fully compliant with HIPAA/HITECH regulations and has reviewed applicable FISMA standards contained in NIST 800-53 and applied them.

2. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

2.1. Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of CMS data files.

The State of Vermont Green Mountain Care Board (GMCB) will use the policies and procedures already stipulated in state regulations and detailed in the "Vermont Healthcare Claims Reporting and Evaluation System: Policies and Procedures Manual for Data Release, Security and Protection" for the state-mandated all payer claims data base that includes commercial and Medicaid data. With the addition of CMS data, additional refinements were made to the manual (final version will include the final CMS DUA) that incorporate the conditions of use and security requirements of CMS as specified in the RIF Data Use Agreement and State DUA Attachment A. The updates to the manual include direct references to the CMS DUA and Attachment A including federal standards. In response to federal standards, we have instituted a new requirement for authorized data users to file Hardware Chain of Custody forms for tracking physical and electronic locations of released data for purposes of accountability, auditing, and to support a final accounting of data location and final disposition for Certificates of Disposition.

GMCB will only release CMS data files to its own contractors or other Vermont state agencies and contractors working under the direction of and funded by the other Vermont state agency after a thorough review of detailed requests for the Medicare data to determine whether the proposed research is compatible with the research activities described in this Executive Summary and the CMS DUA. We also note in the manual that the default files for authorized users will be de-identified and that requests to use files with PII will require additional review by GMCB in consultation with CMS. Requesting state agencies will be required to file data use agreements with GMCB, notarized data user affidavits, and

Hardware Chain of Custody forms from every individual with access to the CMS data agreeing to meet all the security requirements and conditions of use and final disposition as specified in the CMS State DUA and State DUA Attachment A. Data will be transmitted from CMS directly to Onpoint Heath Data as the primary data custodian identified in the CMS DUA for data processing and management. Any additional sharing and distribution of CMS data files will be limited to Vermont state agencies and their designated contractors performing work directed and funded by the state as authorized by GMCB under this process including signed agreements that other data recipients meet CMS and state standards and regulations for data security. Per the response to 2.2, any transmission from Onpoint Health Data to other authorized users will be limited to secure delivery of files on physical media and not transmitted or accessed electronically at this time.

2.2. Please indicate how you will allow other state agencies (and /or contractors) access the data files:
__ VPN connection
__ Requesting organization will travel to physical location of data files
X A copy of the data files be housed at second location
X Other: VPN access is a consideration for the future if funding and adequate technological capacity is secured. Under this application and DUA for CMS data, second locations will have to comply with CMS security requirements and Green Mountain Care Board (GMCB) privacy standards and regulations.

2.3. If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to (e.g., secure web transfer, encrypted hard drives) and secured at (e.g., collection of a data management plan, DUA between state agencies) this location.
Under a CMS DUA for State Agencies, Onpoint Health Data to be the primary Data Custodian for GMCB as the Requestor. Onpoint Health Data has a secure facility and security procedures and will receive the data directly from CMS to process and manage. If GMCB approves release of CMS data from Onpoint to other Vermont state agencies or designated state contractors working for Vermont state agencies, data recipients will be required to file agreements and data user affidavits with DFR that include agreement to meet data management and security requirements as specified by CMS and GMCB.

3. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

3.1. In the event that the state is required by CMS to stop all research activities with CMS data, describe your organization's process to complete the Certificate of Data Destruction form and policies and procedures to destroy data files.

GMCB will use the policies and procedures stipulated in the updated "Vermont Healthcare Claims Reporting and Evaluation System: Policies and Procedures Manual for Data Release, Security and Protection" addressing the process for Certificates of Disposition and standards to be followed by the Principal Investigator/State Agency to destroy and/or discard the data files, electronic data, physical data, derivatives and subsets of data files (Sections II-d, II-e, III-d, III-e, Attachments 6, 7, 8, 9). The GMCB Director of Analysis and Data Management (Dian Kahn at dian.kahn@state.vt.us and (802) 828-2906) will provide oversight for completion of VHCURES Certificates of Disposition and will return the CMS Certificate of Disposition to CMS pertaining to the destruction and/or discarding of CMS Medicare data, derivatives and subsets of the data files. As described in the manual, this process will also require timely and final filings of Hardware Chain of Custody forms by authorized users/principal investigators to GMCB. The manual will be updated to include the final signed CMS DUA if and when obtained.

3.2. In the event that the state is required by CMS to stop all research activities with CMS data, describe your organization's policies and procedures to ensure original data files are not used following notice from CMS.

In the updated "Vermont Healthcare Claims Reporting and Evaluation System: Policies and Procedures Manual for Data Release, Security and Protection" addressing the process for Certificates of Disposition and data destruction standards and procedures (Sections II-d, II-e, III-d, III-e, Attachments 6, 7, 8, 9), the Principal Investigator/State Agency will ensure that authorized (and non-authorized) users will not retrieve or have access to CMS data (e.g., original data files, physical copies, electronic data, aggregate data) files stored at Onpoint or any other organization upon revocation or natural termination of every data use agreement. Dian Kahn, the GMCB Director of Analysis and Data Management will oversee the filings and filing reviews to confirm that the data have been properly destroyed per the standards cited in Attachment 9 of the manual. Ms. Kahn or any GMCB employee charged with this responsibility in the future will not only send Email confirmation to the Data Custodian but also to every data user who filed a Data Users Affidavit (Attachment 5 in the manual). Ms. Kahn maintains a data users contact database and communicates with data users on a regular and continuous basis regarding data use policies and procedures.

According to state and federal standards, the data at every location will be destroyed via pneumatic hammer destruction, degaussing, or application of destruction/deletion technologies that render the data unrecoverable. This will all be documented in the Hardware Chain of Custody form (Attachment 6) to be filed with GMCB with every Certificate of Disposition (Attachment 7).

LOG OF STATE AGENCIES AND OTHER ORGANIZATIONS USING CMS DATA

This section specifically identifies each state agency or organization that will be using the data or seeing individual level results. This log must be supplied to CMS on a quarterly basis.

State Department (or contractor)	Summary of Research Plans Using Medicare Data	Access Method*
Green Mountain Care Board (GMCB)	Administers the VHCURES APCD program and the contract with the Data Custodian for processing, mapping, integrating, and managing the data. Develops state health care expenditure analysis; identify macro trends in health spending; decomposition of cost drivers. Develops population based capacity to support studies of adjusted and unadjusted small area/population variations in utilization, markets, spending, health outcomes. Will conduct special studies on primary care. What-if predictive modeling for VT population.	GMCB does not manage record-level data in-house. GMCB manages a contract with Onpoint Health Data to process, integrate, and manage the data in a secure data warehouse. GMCB as the Requestor/User in the CMS data use agreement will review and approve or deny requests for record-level data and proposals for reporting generated from the VHCURES data warehouse. GMCB will release CMS data to its contractors to perform work directed by GMCB and funded by the State of Vermont. GMCB contractors are required to comply with policies and procedures for data access, security and protection of privacy.
Onpoint Health Data	DUA Data Custodian and GMCB contractor for collecting, processing, integrating, and consolidating data and	Data released by CMS under this DUA will be stored by Onpoint Health Data as described under sections 1.1 and 1.2.

	managing the VHCURES APCD data warehouse. May produce de-identified aggregate reports as requested by GMCB for evaluation of data completeness and quality.	Onpoint Health Data will be authorized to use the data as a state agency contractor for GMCB and other state agencies as approved by GMCB and limited to uses permitted under the CMS DUA that also comply with federal and state laws and regulations.
Truven Health Analytics	Analytics contractor for GMCB. See Summary of Research Plans for GMCB.	GMCB will approve release of CMS data to Truven Health Analytics as a designated GMCB contractor to perform work directed by GMCB and funded by the State of Vermont. All members of the Truven project staff with access to the data will file notarized data user affidavits with GMCB attesting to meet CMS security requirements and to comply with conditions of use and public reporting guidelines as specified in CMS DUA and Attachment A.
Department of Vermont Health Access (DVHA)	Data will be used to conduct analytics in support of the models to be tested under the State Innovation Model grant from CMMI. The analytics will include but not limited to: policy analysis, economic modeling, program development, performance benchmarking, outcomes studies and evaluations of interventions.	GMCB will review and authorize release of CMS data to DVHA and its contractors to perform work directed and funded by the State of Vermont. DVHA and contracts will meet DUA requirements and comply with GMCB policies and procedures for data security and protection of privacy. Data transfer will be done in a secure manner consistent with GMCB requirements. GMCB will monitor and track data access and use that will be documented.

*If the data will be housed in a separate location from that identified in the DUA, please note the separate location here

DISSEMINATION AND REPORTING OF FINDINGS

Please describe your plans for disseminating the findings from your analysis, including specific media through which you will report results.

The CMS data will be used for internal analyses by the State and for the publication of statistics and reports pertaining to health care reform and health programs as described in the Executive Summary. The reports will comply with HIPAA

CMS rules pertaining to keeping the data de-identified through the absence of PHI data fields and suppression of cells with fewer than 11 cases in public reports or any reports subject to public records requests. The reports will be used primarily for system metrics, policy analysis and program evaluation and will pose minimal risk upon individuals and for identification of individual beneficiaries.