Application for

Requesting Health Care Claims Research Data Sets

Office of Health Strategy All Payer Claims Database ("APCD") requires data requestors to complete this application to request access to APCD data. This application is only for de-identified data sets, which conform to the HIPAA Privacy Rule 45 CFR 164.514 (a)-(b) with members de-identified to protect privacy.

Please note that some parts of your completed application will be publicly posted on the APCD's website. Research Methodology and Data Security details will not be posted publicly.

Please complete the application form below to request access to the APCD data. The APCD Data Review Committee (DRC) will evaluate all requests. Please submit your data request application, additional documents and/or spreadsheets and any questions to:

Attn: Data Request Application, APCD

OHS.APCD@ct.gov

1. GENERAL INFORMATION

Applicant Information	Details
Principal Investigator's Name and Title:	Dr. Chima Ndumele, Associate Professor of Public Health (Health Policy) and Associate Professor in the Institute for Social and Policy Studies
Organization Name:	Yale University
Street Address, City/Town, State, Zip Code:	60 College St. New Haven, CT 06520
E-mail:	chima.ndumele@yale.edu
Phone Number:	203-737-3379
Date of Application (MM/DD/YYYY):	(09/01/2021)
Project / Research Title:	Understanding Trends in Healthcare Use, Cost, and Outcomes for Populations with Chronic Conditions
Project / Research Objective(s) (100 words or less):	First, we will investigate whether trends in use of care, cost of care, and intermediate health outcomes exist among CT residents with chronic conditions who are privately insured.

	Second, we will estimate the relationship that exists between use of care, cost of care, and intermediate health outcomes for this population. Third, we will explore whether disparities exist in both the trends or relationships between use of care, cost of care, and intermediate health outcomes across gender, race, ethnicity, poverty-level, employment sector, and geography (county) for CT residents with chronic conditions.
Project / Research Question(s) to be addressed via proposed research (if applicable, briefly)	1. What trends exist in the use of care, cost of care, and intermediate outcomes among CT residents with chronic conditions? 2. What relationship exists between use of care, cost of care and intermediate outcomes among CT residents with chronic conditions? 3. What disparities exist in these trends and relationships across gender, race, ethnicity, poverty-level, employment sector, and geography (county) for CT residents with chronic conditions?
Contact Name:	Chima Ndumele
Contact Phone Number:	203-737-3379
Contact E-Mail:	chima.ndumele@yale.edu
Others Accessing Data:	1. Dr. Jacob Wallace 2. Dr. Anthony Lollo 3. Matthew Lavallee 4.

2. PROJECT SUMMARY

Briefly describe the purpose of this project and how the requested data from Connecticut's APCD will accomplish your purpose.

Brief overview of research project (in 200 words or less): The proposed project looks to explore trends in use of care, cost of care, and intermediate health outcomes for privately insured CT residents living with chronic conditions. Additionally, the project will estimate the relationship between use of care, cost of care, and intermediate health outcomes, along with searching for disparities across gender, race, ethnicity, poverty-level, employment sector, and geography (county). The results of this research will examine access and processes of care for a vulnerable population (chronically-ill), and shed light on how that care may vary across gender, race, ethnicity, poverty-level, employment sector, and geography (county).

Connecticut's APCD is an essential component for this work, as it offers some of the most complete claims data for CT's privately insured residents.

3. RESEARCH PROTOCOL

Please fill-in the following information.

A. Summary of background, purposes and origin of the research (in 200 words or less):

Chronically ill populations are an important group that incur great health care costs, often require increased care and are at increased risk of adverse outcomes. Understanding the way these populations receive care, and how that care has changed over time, offers important insight for improving health outcomes for these populations. Additionally, disparities in healthcare and health outcomes remain for general populations. Understanding if and how disparities exist for chronically ill populations across gender, race, ethnicity, poverty-level, employment sector, and geography (county) could offer valuable information on where policymakers and payers should target their efforts in improving delivery of care and health outcomes.

B. How does the research address health-related questions, particularly in the context of improving health and health equity? (in 100 words or less):

This work has the potential to not only shed light on inequalities that may exist within privately insured chronically-ill populations, but also offer recourse by exploring the potential relationships between use, cost, and outcomes in healthcare, and those inequalities across gender, race, ethnicity, poverty-level, employment sector, and geography (county). This research will be instrumental in shaping care for chronically-ill populations across a variety of social determinants.

C. Please describe research design and methodology (in 200 words or less):

Our study will create measures of high-value care and examine acute hospitalizations among chronically ill individuals in CT. We will use multiple regression techniques and risk adjustment to better understand variation in the receipt and use of services among the chronically ill. We will also examine whether high-value and low-value services are compliments or substitutes for each other among this population. Finally, we will try and examine which demographic groups (e.g. racial/ethnic) are more or likely to receive high/low value services among the chronically ill. We will create measures of effective (high-value) care from the NCQA HEDIS specifications

D. Expected begin and end dates of the research:

Expected Start: (10/1/2021)
Expected End: (10/1/2024)

E. Organizational qualifications: Briefly describe your organization's experience with projects of similar scale and scope:

We have assembled an interdisciplinary team that brings together health policy experts, health economists, social science researchers, and practitioners with experience in Medicaid, social determinants, programmatic design, and the construction and analysis of large data sets. We have done similar work using detailed health insurance claims from state Medicaid agencies and large survey data. **Chima Ndumele, PhD** (Principal Investigator) is an Associate Professor of Health Policy at the Yale School of Public Health. His research primarily focuses on the role of delivery systems in improving health care access and outcomes for low-income populations. Dr. Ndumele has conducted several studies on the provision of services in Medicaid and the relationship between social services and health outcomes.

F. Funding Source:

What is the funding source of this project?
Yale School of Public Health (Internal)

What is the duration of this funding?
N/A

Do you intend to charge a fee for your reports or the results of your analyses?
No

If yes, to whom?

Click or tap here to enter text.

G. Prior Review:

You are required to allow APCD's administrator to review your report or output (spreadsheet, data table, etc.) prior to any publication to ensure that the report is in compliance with the requirements for attributes, including cell suppression rules, risk of inferential reidentification, and consistency to methodology of the project. Please describe how you intend to comply with this requirement.

We will submit output for review at least 4 weeks prior to the submission for publication

On what date do you expect to release/publish this report?

12/31/2022 (estimated)

By what date do you intend to file it with APCD's administrator? (at least 4-week review period needed)

11/28/2022 (estimated)

4. Data Selection(s)

A. Data sets – each type of data set will have one standard format unless the requestor wants to customize it further (at additional cost.) The data sets are -

- Eligibility
- Medical Claims
- Pharmacy Claims
- Inpatient Discharge Data
- ED Data
- Outpatient Facility Data
- Professional Data

B. Filters

Applicants can request filters on the data for limited extraction, if necessary for their research project. A list of common filters is given below.

Common Filters	Data Set	Requested Filter
Eligibility		None
Medical Claims		None
Pharmacy Claims		None
Inpatient Discharge Data		None
ED Data		None
Outpatient Facility Data		None
Professional Data		None
		Click or tap here to enter text.
		Click or tap here to enter text.

C. Aggregated Data

Applicants can request that data is aggregated into summary tables. Doing so will provide an applicant with total counts, average, standard deviation, rates, and other meaningful statistical measures. Applicants will have to provide information on the following tables.

Data Set or Field Names	Count, Sum, Average, Dev, Range, Rate	Description of Summary	Group By Variable(s)
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

5. DATA SECURITY AND INTEGRITY

(Information from this section will not be posted on the APCD's public website.)

Please see the attached data management plan which outlines our process for securing storing, analyzing, transferring and destroying data

1. Where will be the data be located physically? (Provide the delivery address for the data including building and floor.)

60 college street, New Haven, Floor 3

2. Please provide name and information of the organization that will host and manage APCD data, including the name of the custodian.

The Principal Investigator (PI), Chima Ndumele, Assistant Professor at the Yale University School of Public Health and Institute for Social and Policy Studies is responsible for organizing, storing and archiving the data.

Yale Information Technology Services (ITS) will provide the PI with a secure server in a secure data center.

3. Describe how you will maintain an inventory of APCD data, derived analytic files and scratch files, and how you will manage physical access to such data during the duration of the project. (Please describe and attach documents supporting your policies and procedures.)

The Principal Investigator (PI), Chima Ndumele, Assistant Professor at the Yale University School of Public Health and Institute for Social and Policy Studies is responsible for organizing, storing and archiving the data.

Yale Information Technology Services (ITS) will provide the PI with a secure server in a secure data center.

Yale University Office Information Security Policy and Compliance (OISPC) maintains an inventory database of all above-threshold systems and a compliance management system which contains all risk assessment documents created during the risk assessment process.

OISPC does not maintain data on the source of externally sourced ePHI data— this is the responsibility of the PI.

HIPAA Policy 5142 Information System Activity Review and HIPAA Procedure 5142 PR.1 Information Systems Activity Review account for audit and review of systems containing electronic protected health information (ePHI).

Policy 5142 ensures that systems containing electronic protected health information (ePHI) are identified, appropriately categorized, monitored and reviewed to ensure compliance with institutional policies and procedures and Federal HIPAA regulations related to system activity controls, and to discourage, prevent and detect security violations

Procedure 5142 accounts for the mechanics of Identifying and tracking Above Threshold ePHI Systems connected to the Yale University Data Network by procedures such as: registration forms to be completed before connection of devices, scanning the network for connected devices, network based registration systems e.g. Ethernet MAC address data base or future implementations, and identification of Above-Threshold System Administrators as part of auditorium and web-based training sessions. Entries in the Above-Threshold ePHI Systems Inventory Database are updated yearly by the responsible system administrators or data owners.

4. Do you have confidentiality agreements with the principal investigator, the data custodian or other research individuals or technical (IT) team members, particularly those with access to the APCD data? (Please describe and attach documents supporting your policies and procedures.)

By using Yale IT resources, users agree to the IT Appropriate Use Policy (Yale Policy 1607, see, http://policy.yale.edu/policies)

5. Technical Safeguards:

   a) Describe the steps do you have to physically secure data, such as site or office access controls, secured file cabinets, and locked offices?

Yale University has an extensive set of policies for the handling, viewing, storing, etc. of protected health information (PHI) in electronic and paper formats. Below is a list of the policies and their titles. The full text of the HIPAA policies are available on the Yale University website at the following address -- http://hipaa.yale.edu/ .

- • 5100 – Security and Health Information – provides the overall approach to HIPAA Security management and includes the Master Glossary of HIPAA Security Terms used in the related set of policies and procedures
- • 5111 – Physical Security Policy – describes how to maintain physical security of ePHI Systems

o 5111 PR.1, 5111 PR.2 – physical security procedures
• 5123 – Electronic Communication of Health Related Information – policy governing

electronic communications of ePHI
o 5123 PR.1 – ePHI messaging procedures

• 5142 – Information Systems Activity Review – how Yale monitors and reviews the activity of ePHI Systems

o 5142 PR.1 – procedure to guide the Systems activity review

- • 5143 – IT Security Incident Response Policy – how clients report IT Security incidents,

  including those involving ePHI, and how the University will respond

- • Other related HIPAA Policies include (http://hipaa.yale.edu/policies- procedures-forms):

o 5001 -- Notice of Privacy Practices
o 5002 -- Right to Request Access and Amendment to Designated Record Set
o 5003 -- Accounting for Disclosures
o 5004 -- Request Restrictions or Confidential Communications
o 5005 -- Reporting Incidents Involving the Security or Privacy of Protected Health

Information; Breach Notification
o 5020 -- Disciplinary Policy for Violations of the Privacy or Security of Protected

o 5026 -- Reporting Protected Health Information (PHI) Compliance Issues
o 5031 -- Authorization Requirements for Use and Disclosure of Protected Health

Information, Including Verification of Identification
o 5032 -- Use and Disclosure of Protected Health Information for Research Purposes o 5033 -- Disclosure of PHI to Business Associates
o 5034 -- Uses and Disclosures of PHI for Marketing
o 5035 -- Uses and Disclosures of PHI for Fundraising
o 5036 -- Transmission and Receipt of Protected Health Information via Fax
o 5037 -- Minimum Necessary Uses, Disclosures, and Requests
o 5038 -- Personal Representatives

o 5039 -- Use and Disclosure of De-Identified Information and of Limited Data Sets o 5040 -- Uses and Disclosures of Genetic Information for Underwriting Purposes

• Other related IT Security Policies (http://policy.yale.edu)
o 1601 – Information Access and Security – describes who can access information

systems, including ePHI Systems
♣ 1601.1 Authorization to Grant or Revoke Access to University Information

- • 1601 PR.02 NetIDs and Identity Management
- • 1601 PR.03 Access Control for Protected Health Information (PHI)
- • 1601 PR.04 VPN Eligibility & Access Procedure
- • 1601 PR.07 Identity Data Access Requests

o 1607 – IT Appropriate Use Policy (Yale's core IT policy)
o 1609 – Media Controls- protecting confidential information, including ePHI

♣ 1609 PR.1 - associated procedure
o 1610 – Systems and Network Security – describes how to maintain IT security of

information systems other than ePHI systems.

- • 1610 PR.1 - best practice computer security guidelines for devices

  without ePHI

- • 1610 PR.2 - disposal of computers

b) What safeguards are in place to restrict data access among the research team? Describe your password-protected access system?

Yale University Information Technology Services maintains secure data center facilities for servers. The data centers are in buildings with a security guard in attendance 24/7 and after normal business hours require both key card entry and written sign-in with the security guard.

Access to data center rooms is restricted to specific identified data center employees and access is controlled by key card. All others persons, both Yale affiliated and non-Yale affiliated, requiring access to a data center to perform work (e.g. hardware vendors, electrical contractors, general maintenance workers, etc.) are accompanied by an authorized data center employee for the duration of their presence in the data center; and must manually sign-in upon entry to the data center.

Each member of the Yale community is assigned a unique network identification credential (NetID). An active NetID and password (passwords are selected by the community member and subject to the guidance in Policy 1610, Guide.01, Selecting Good Passwords) controls access to the university network while on campus or via VPN and MFA (Multi-factor authentication) when off campus.

c) Describe your policies and procedures for ensuring APCD data is protected while stored on server(s). Describe how your organization ensures that APCD data on servers cannot be copied to local workstations, laptops, smartphones, and other media (CDs, DVDs, hard drives, thumb drives, etc.).

All users must connect using Yale credentials (NetID). All users must be granted permission to access the data; Yale NetID holders who have not been granted this access are prevented from connecting to this resource. For users connecting remotely, multi-factor authentication (MFA) is required for VPN connections. VPN connections are secured by IPSEC. Next generation network security devices protect all data center assets and are set to alert or automatically drop network traffic depending on the nature of a security event.

d) Provide your organization's written information security program (WISP) or its policies & procedures regarding security provisions, particularly security or privacy safeguards against unauthorized access to or use of health data.

Yale University Information Technology Services maintains secure data center facilities for servers. The data centers are in buildings with a security guard in attendance 24/7 and after normal business hours require both key card entry and written sign-in with the security guard.

Access to data center rooms is restricted to specific identified data center employees and access is controlled by key card. All others persons, both Yale affiliated and non-Yale affiliated, requiring access to a data center to perform work (e.g. hardware vendors, electrical contractors, general maintenance workers, etc.) are accompanied by an authorized data center employee for the duration of their presence in the data center; and must manually sign-in upon entry to the data center.

Each member of the Yale community is assigned a unique network identification credential (NetID). An active NetID and password (passwords are selected by the community member and subject to the guidance in Policy 1610, Guide.01, Selecting Good Passwords) controls access to the university network while on campus or via VPN and MFA (Multi-factor authentication) when off campus.

Logical access to the server that houses the APCD data files will be controlled by NetID and set by an Active Directory (AD) group. NetID's within the AD group (as authorized by the PI) will connect and log into to the server housing the APCD data files. The server is likely to be part of a multi-tenant virtual machine which controls in place to ensure privacy and security between environments.

6. SIGNATURES

By signing this application, you certify that the information enclosed herein is true and correct and if this Application is approved you agree to the terms and conditions of the Data Use Agreement (DUA) for the use of the APCD Data.

For the Applicant:
Signature:

Name: Chima Ndumele
Title: Associate Professor of Health Policy
Date: 9/1/21
Organization: Yale School of Public Health

APPENDIX 1: SPECIFICATIONS FOR DATA RELEASE APPLICATION

General Information & Instructions

1. The APCD may deliver data via the following options:
    a. Secured File Transfer: An approved applicant will be allowed to access data at approved levels for an established time period.
    b. Disk drives: An approved applicant will be allowed to access data encrypted on a device – DVD drives, CD drives or Disk / USB Flash drive.
2. For data filters, use Table 4(B) to select filters from Eligibility, Medical, and Pharmacy claims.
3. For summary data, applicant will have to specify on Table 4(C) in the application and/or work closely with APCD's staff to ensure accuracy of the methodology.
4. Associated fees must be received prior to issuing access credentials to the Applicant. See data access fee schedule for information about access fees.
5. An APCD data dictionary is available on the APCD website (https://healthscorect.com/researcher#dictionary).

APPENDIX 2: Certification of Project Completion, Destruction, or Retention of Data

Name:	
Title:	
Organization:	
Address:	
Telephone:	
E-mail:	
Project Title:	
Data Sets:	
Years:	
☐ Certification of data Destruction – date when data destroyed:	
☐ Request to Retain Data	Date until data will be retained:

I hereby certify that the project described in the applications is complete as of ___/___/20__. Please select one or more of the following options:

☐I/We certify that we have destroyed all data received from the APCD in connection with this project in any media, form, or format. This includes but is not limited to: data maintained on hard or USB flash drive(s), DVDs/CDs, or any other printed materials.

☐I/We certify that we have retained all data received from the APCD's administrator in connection with this project, pursuant to the following health or research justification (provide detail on why it is necessary to retain data and for how long:

_____
_____

☐I/We certify that we have retained all Data received from APCD's administrator in connection with this project, as required by the data use agreement.

_____
_____

SIGNATURE:

For the Receiving Organization: _____
Date: _

CT APCD Data Release - Table & Field Requests

Table Name	1) Please Indicate Which Tables Will Be Needed	Reason
Eligibility	Requested	Our analysis will require detailed information about enrollee characteristics in order to understand trends within groups, and differences between groups.
Eligibility Supplemental	Requested	It will be valuable to have the extended demographics around employment status and type for understanding trends among the privately insured.
Medical	Requested	It will be necessary for us to have information on medical claims in order to assess trends in care, specifically approximate dates and place of service will be important.
Medical Claim Header	Requested	It will be important for us to have additional information on the claims, including information on claim status, length of stay, and payments.
Medical Supplemental	Requested	It would be useful for us to have the extended information, like whether or not a claim was in network or whether or not a claim was with the PCP.
Medical Claim Diagnosis	Not Requested	
Medical Claim Icd Procedure	Not Requested	
Pharmacy	Requested	Having information on the drugs prescribed the patients will be vital for understanding trends in quality of care.
Pharmacy Supplemental	Requested	It will be valuable for us to have extended information on pharmacy claims, including how much patients paid.
Provider	Requested	Having provider NPIs will be important to assessing trends in types of care (i.e. care with specialists).

Variable Classes	2) Please Indicate Which Variable Classes Will Be Needed	Reason
Administrative	Requested	Administrative data may be necessary for linking claims.
Enrollee Coverage Information	Requested	Enrollee characteristics will be important for understanding trends in care within and between groups
Enrollee Demographics	Requested	Enrollee characteristics will be important for understanding trends in care within and between groups
Claim Information	Requested	It will be necessary to detailed information on the claims to understand trends in care.
Diagnosis Information	Requested	It will be necessary to detailed information on the claims to understand trends in care.
Procedure Coding & Detail	Requested	It will be necessary to detailed information on the claims to understand trends in care.
Financial Information	Requested	Information on expenses related to care will be valuable in understanding differences between groups.
Provider Information	Requested	Provider information will be important in assessing trends in types of care (i.e. care with specialists).
Payer Information	Requested	Having the submitter ID could prove important.
Safe Harbor Variable	Requested	It will be necessary for us to have details like gender, and ZIP for assessing enrollee trends.

Data sets & Filters – each type of data set will have one standard format unless the requestor wants to customize it further at additional cost

Dataset/Common Filters	3) Data Set/Filter	Indicate Data set and/or Filter For Data Extract (Provide as much detail as possible)
Eligibility	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Medical Claims	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Pharmacy Claims	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Inpatient Discharge	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
ED Visits	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Outpatient	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Professional	Data Set	**Only interested in private enrollees (no Medicaid), from 2013-2020**
Eligibility Dates	Eligibility	Only interested in private enrollees (no Medicaid), from 2013-2020
Members' Age	Eligibility	Only interested in private enrollees (no Medicaid), from 2013-2020
Members' Gender	Eligibility	Only interested in private enrollees (no Medicaid), from 2013-2020
Zip Codes	Eligibility	Only interested in private enrollees (no Medicaid), from 2013-2020
Inpatient Admissions	Medical	Only interested in private enrollees (no Medicaid), from 2013-2020
Procedures Codes (ICD/CPT/HCPCS)	Medical	Only interested in private enrollees (no Medicaid), from 2013-2020
Service Dates	Medical	Only interested in private enrollees (no Medicaid), from 2013-2020
Diagnoses Codes (ICD)	Medical	Only interested in private enrollees (no Medicaid), from 2013-2020
Medications (NDCs)	Pharmacy	Only interested in private enrollees (no Medicaid), from 2013-2020

Prescription Filled Date	Pharmacy	Only interested in private enrollees (no Medicaid), from 2013-2020
Taxonomy codes	Provider	Only interested in private enrollees (no Medicaid), from 2013-2020
Add rows for others		

DATA MANAGEMENT PLAN[1]

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

For research studies involving researchers from another organization that will have access to RIF or non-identifiable files, please refer to the Collaborator Checklist for guidance and considerations to include in the Data Management Plan.

For collaborating organizations that will be receiving a physical copy of the CMS data files, a full Data Management Plan should be completed by the collaborating organization.

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).

The Principal Investigator (PI), Chima Ndumele, Assistant Professor at the Yale University School of Public Health and Institute for Social and Policy Studies is responsible for organizing, storing and archiving the data.

Yale Information Technology Services (ITS) will provide the PI with a secure server in a secure data center.

1.2. Describe how your organization maintains a current inventory of CMS data files.

The Principal Investigator (PI), Chima Ndumele, Assistant Professor at the Yale University School of Public Health and Institute for Social and Policy Studies is responsible for organizing, storing and archiving the data.

Yale Information Technology Services (ITS) will provide the PI with a secure server in a secure data center.

Yale University Office Information Security Policy and Compliance (OISPC) maintains an inventory database of all above-threshold systems and a compliance management system which contains all risk assessment documents created during the risk assessment process. OISPC does not maintain data on the source of externally sourced ePHI data— this is the responsibility of the PI.

[1] Note that CMS is specifically asking for reference to written policies and procedures related to your organization's administrative, technical and physical safeguards. If policies and procedures have not been developed, please explain any ongoing activities your organization is taking to document and make them available to staff. Organizations selected for DPSP reviews will be asked to provide copies of written policies and procedures. Please note that an explanation of the process is not sufficient.

HIPAA Policy 5142 Information System Activity Review and HIPAA Procedure 5142 PR.1 Information Systems Activity Review account for audit and review of systems containing electronic protected health information (ePHI).

Policy 5142 ensures that systems containing electronic protected health information (ePHI) are identified, appropriately categorized, monitored and reviewed to ensure compliance with institutional policies and procedures and Federal HIPAA regulations related to system activity controls, and to discourage, prevent and detect security violations

Procedure 5142 accounts for the mechanics of Identifying and tracking Above Threshold ePHI Systems connected to the Yale University Data Network by procedures such as: registration forms to be completed before connection of devices, scanning the network for connected devices, network based registration systems e.g. Ethernet MAC address data base or future implementations, and identification of Above-Threshold System Administrators as part of auditorium and web-based training sessions. Entries in the Above-Threshold ePHI Systems Inventory Database are updated yearly by the responsible system administrators or data owners.

1.3. Describe how your organization binds all members (i.e., organizations, individual staff) of research teams to specific privacy and security rules in using CMS data files.
By using Yale IT resources, users agree to the IT Appropriate Use Policy (Yale Policy 1607, see, http://policy.yale.edu/policies)

1.4. Provide details about whom and how your organization will notify CMS of any project staffing changes.
The PI is responsible for notifying CMS of project staffing changes. The PI has developed a written procedure for notifying CMS of staffing changes. The procedure will be kept on file by the PI and made available to CMS and OISPC upon request.

1.5. Describe your organization's training programs that are used to educate staff on how to protect CMS data files.
The Yale University HIPAA Privacy and Security Training is delivered electronically. The training content and the training modules are managed by the Yale University HIPAA Privacy Office.

By policy all members of the Yale University community, including researchers, who work or train in those parts of the university that provide health care and health care benefits or in offices that provide support or advice related to health care or do research about health or healthcare must complete HIPAA Privacy and Security Training.

Each year all Faculty, staff, postdoctoral fellows and postdoctoral associates are required to complete an online assessment designed to help employees at Yale identify federal, state and University training and form submission requirements.

Upon completion of the online assessment a list of training requirements (which may include certain forms) will display within the "Requirements" section of the Training and Certification Website.

Additional guidance on data security topics can be found on the website of Yale's Information Technology Services (http://its.yale.edu).

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

The data will be secured in a Yale University Information Technology Services (ITS) data center. The data will be stored on a file server executing Windows Server 2012 running in [a multi-tenant virtual environment or an individual physical server]. Devices in the ITS data center are assigned private IP addresses and network address translation (NAT) is used to provide access to the Internet when necessary. Yale has perimeter defenses in place to protect both the data center networks and the Yale network as a whole from malicious actors.

1.7. Describe the policies and procedures regarding the physical possession and storage of CMS data files.

Yale University has an extensive set of policies for the handling, viewing, storing, etc. of protected health information (PHI) in electronic and paper formats. Below is a list of the policies and their titles. The full text of the HIPAA policies are available on the Yale University website at the following address -- http://hipaa.yale.edu/ .

- **5100 – Security and Health Information** – provides the overall approach to HIPAA Security management and includes the Master Glossary of HIPAA Security Terms used in the related set of policies and procedures
- **5111 – Physical Security Policy** – describes how to maintain physical security of ePHI Systems
    - 5111 PR.1, 5111 PR.2 – physical security procedures
- **5123 – Electronic Communication of Health Related Information** – policy governing electronic communications of ePHI
    - 5123 PR.1 – ePHI messaging procedures
- **5142 – Information Systems Activity Review** – how Yale monitors and reviews the activity of ePHI Systems
    - 5142 PR.1 – procedure to guide the Systems activity review
- **5143 – IT Security Incident Response Policy** – how clients report IT Security incidents, including those involving ePHI, and how the University will respond
- Other **related HIPAA Policies** include (http://hipaa.yale.edu/policies- procedures-forms):
    - **5001** -- Notice of Privacy Practices
    - **5002** -- Right to Request Access and Amendment to Designated Record Set
    - **5003** -- Accounting for Disclosures
    - **5004** -- Request Restrictions or Confidential Communications
    - **5005** -- Reporting Incidents Involving the Security or Privacy of Protected Health Information; Breach Notification
    - **5020** -- Disciplinary Policy for Violations of the Privacy or Security of Protected Health Information

- **5026** -- Reporting Protected Health Information (PHI) Compliance Issues
- **5031** -- Authorization Requirements for Use and Disclosure of Protected Health Information, Including Verification of Identification
- **5032** -- Use and Disclosure of Protected Health Information for Research Purposes
- **5033** -- Disclosure of PHI to Business Associates
- **5034** -- Uses and Disclosures of PHI for Marketing
- **5035** -- Uses and Disclosures of PHI for Fundraising
- **5036** -- Transmission and Receipt of Protected Health Information via Fax
- **5037** -- Minimum Necessary Uses, Disclosures, and Requests
- **5038** -- Personal Representatives
- **5039** -- Use and Disclosure of De-Identified Information and of Limited Data Sets
- **5040** -- Uses and Disclosures of Genetic Information for Underwriting Purposes

- Other **related IT Security Policies (http://policy.yale.edu)**
  - **1601** – Information Access and Security – describes who can access information systems, including ePHI Systems
    - 1601.1 Authorization to Grant or Revoke Access to University Information
      - 1601 PR.02 NetIDs and Identity Management
      - 1601 PR.03 Access Control for Protected Health Information (PHI)
      - 1601 PR.04 VPN Eligibility & Access Procedure
      - 1601 PR.07 Identity Data Access Requests
  - **1607** – IT Appropriate Use Policy (Yale's core IT policy)
  - **1609** – Media Controls- protecting confidential information, including ePHI
    - 1609 PR.1 - associated procedure
  - **1610** – Systems and Network Security – describes how to maintain IT security of information systems other than ePHI systems.
      - 1610 PR.1 - best practice computer security guidelines for devices without ePHI
      - 1610 PR.2 - disposal of computers

1.8. Explain your organization's system or process to track the status and roles of the research team.

Yale University faculty, staff and other employees are managed through Workday, a human resources management system while students are managed through Yale's student management system. Yale NetIDs are managed centrally through an identity and access management system. Upon termination, at graduation, or at the direction of a supervisor, access to systems via NetID can be suspended or terminated.

The PI is will track the status and roles of the research team. The PI will provide written documentation to CMS listing the individuals who can access the CMS data housed at Yale. These authorized individuals will use their Yale unique credentials (NetID) to access the secure server that contains the CMS data files.

The PI will provide written notification (via email or Yale ITS's internal ticketing system) to the Yale Windows System Team (the team responsible for administrating the windows servers at Yale University) with instructions to remove any individuals no longer working on CMS data projects. The

PI will be notified in writing (via email or Yale ITS's internal ticketing system) when access has been removed.

Yale University Policy 1601 Information Access and Security, its sub-policies and procedures establishes requirements for staff, faculty and students regarding access to University information as well as the responsibilities for stewardship of University information. University information is all information generated or acquired, in printed or digital form, by Yale faculty, staff, students, contractors or others engaged on the University's behalf, in the course of carrying out the University's mission or conducting its business.

1.9. Describe your organization's physical and technical safeguards used to protect CMS data files (including physical access and logical access to the files).

Yale University Information Technology Services maintains secure data center facilities for servers. The data centers are in buildings with a security guard in attendance 24/7 and after normal business hours require both key card entry and written sign-in with the security guard.

Access to data center rooms is restricted to specific identified data center employees and access is controlled by key card. All others persons, both Yale affiliated and non-Yale affiliated, requiring access to a data center to perform work (e.g. hardware vendors, electrical contractors, general maintenance workers, etc.) are accompanied by an authorized data center employee for the duration of their presence in the data center; and must manually sign-in upon entry to the data center.

Each member of the Yale community is assigned a unique network identification credential (NetID). An active NetID and password (passwords are selected by the community member and subject to the guidance in Policy 1610, Guide.01, Selecting Good Passwords) controls access to the university network while on campus or via VPN and MFA (Multi-factor authentication) when off campus.

Logical access to the server that houses the CMS data files will be controlled by NetID and set by an Active Directory (AD) group. NetID's within the AD group (as authorized by the PI) will connect and log into to the server housing the CMS data files. The server is likely to be part of a multi-tenant virtual machine which controls in place to ensure privacy and security between environments.

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 data will not be shared with any individuals outside of the research team as identified by the PI.

The CMS data files are subject to the policies and procedures regarding protected health information (PHI). Yale University has an extensive set of policies for the handling, viewing, storing, etc. protected health information (PHI) in electronic and paper formats. The HIPAA policies are listed in response to question 1.7

2.2. If your organization employs a data tracking system, please describe.

A data tracking or data loss prevention system will not be used in this environment. All users who are authorized to access the file server will have full access to the dataset. Regular access will be

logged by the Windows Operating System and in a forensic scenario, Yale should be able to reconstruct who accessed to the dataset using system access logs.

2.3. Describe the policies and procedures your organization has developed for the physical removal, transport and transmission of CMS data files.
The following policies and procedures cover all organizational units of Yale University and apply to media in any format that contains confidential information.

- 1609 Media Control Policy and policy sections;
  - 1609.1 General guidelines for media containing confidential information
  - 1609.2 Disposal of media containing confidential information
  - 1609.3 Disposal of media containing confidential information
  - 1609 PR.01 Disposal of Media Containing Confidential or Protected Health Information

Disposal of electronic media containing electronic Protected Health Information is managed by Yale data disposal vendors. Requests for disposal are completed using a Universal Waste Disposal request located on the Yale Website located at http://ehs.yale.edu/universal-waste.

The vendor uses industry standard methods to dispose of electronic media devices for the University and provides certificates of destruction at the end of the destruction process.

The PI has developed a written procedure that prohibits the removal of CMS data to portable media (e.g. optical media, USM mass storage, etc.) or storage on an unencrypted device.

2.4. Explain how your organization will tailor and restrict data access privileges based on an individual's role on the research team.
The PI and his designated research associates will have the same access level to the CMS data files for the purposes of research. Only the PI is authorized to grant access, to his designated research associates, to the CMS data files.

2.5. 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).
All users must connect using Yale credentials (NetID). All users must be granted permission to access the data; Yale NetID holders who have not been granted this access are prevented from connecting to this resource. For users connecting remotely, multi-factor authentication (MFA) is required for VPN connections. VPN connections are secured by IPSEC. Next generation network security devices protect all data center assets and are set to alert or automatically drop network traffic depending on the nature of a security event.

2.6. Are additional organizations involved in analyzing the data files provided by CMS?
No other organizations or individuals from other organizations will have access or be involved in analyzing the data files

If so, please review the Collaborator Checklist for guidance and considerations to include in the Data Management Plan, and indicate below how these organizations' analysts will access the data files:

__ VPN connection
__ Will travel to physical location of data files at requesting organization
__ Request that a copy of the data files be housed at second location
__ Other: Click here to enter text.

2.7. If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location. (Also, please ensure you have included information on this organization's database management under the appropriate subsections of the database management plan.)
No other organizations or individuals from other organizations will have access or be involved in analyzing the data files.

3. **DATA REPORTING AND PUBLICATION**

3.1. Who will have the main responsibility for notifying CMS of any suspected incidents wherein the security and privacy of the CMS data may have been compromised? Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the CMS data.
The HIPAA Privacy Officer of Yale University is responsible for notifying CMS of any suspected incidents wherein the security and privacy of the CMS data may have been compromised. Yale's Office of Information Security, Policy and Compliance (OISPC) maintains an internal Incident Response Policy, which will be followed in the event an incident is suspected. This policy includes a duty to notify the HIPAA Privacy Officer of any events of this nature. It is the PI's responsibility to report any potential security events to OISPC immediately upon discovery.

3.2. Explain how your organization's data management plans are reviewed and approved.
Data management plans are reviewed by OISPC before they are submitted. The PI is ultimately responsible for their content.

3.3. Explain whether and how your organization's data management plans are subjected to periodic updates during the DUA period.
There is currently no policy in place that requires review of the organization's data management plans. During configuration of key systems and during other security checkpoints, Yale's activities will be checked against the requirements in the agreement.

3.4. Please attest to the CMS cell suppression policy of not publishing or presenting tables with cell sizes less than 11. (see Item 9 of the DUA) X I agree.

*The following items are for **Part D requests only**:*

3.5. The researcher agrees that the pharmacy, provider, prescriber, or health plan will not be identified in this study.
__ I agree.

4. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

4.1. Describe your organization's process to complete the Certificate of Disposition form and policies and procedures to dispose of data files upon completion of its research.
There are no specific University processes in place for the completion of the Certificate of Disposition. The PI will be responsible for requesting that IT staff complete it for assets in the data center. The PI is responsible for any media or data stored outside of the central IT infrastructure (e.g. the media on which the data set is delivered from CMS to Yale University).

The following policies and procedures cover all organizational units of Yale University and apply to media in any format that contains confidential information.

- 1609 Media Control Policy and policy sections;
    - 1609.1 General guidelines for media containing confidential information
    - 1609.2 Disposal of media containing confidential information
    - 1609.3 Disposal of media containing confidential information
    - 1609 PR.01 Disposal of Media Containing Confidential or Protected Health Information

Disposal of electronic media containing electronic Protected Health Information is managed by Yale data disposal vendors. Requests for disposal are completed using a Universal Waste Disposal request located on the Yale Website located at http://ehs.yale.edu/universal-waste .

The vendor uses industry standard methods to dispose of electronic media devices for the University and provides certificates of destruction at the end of the destruction process.

4.2. Describe your organization's policies and procedures used to protect CMS data files when individual staff members of research teams (as well as collaborating organizations) terminate their participation in research projects (which may include staff exit interviews and immediate access termination).

The PI has developed procedures to ensure that all assets are returned to the University upon termination of individual staff members of the research team's participation in research projects. Yale Human Resources has specific policy guidelines in place for off-boarding of staff that includes a checklist that helps ensure logical and physical access to research data is prevented after termination.
.

4.3. Describe policies and procedures your organization uses to inform CMS of project staffing changes, including when individual staff member's participation in research projects is terminated, voluntarily or involuntarily.
The PI is will track the status and roles of the research team. The PI will provide written documentation to CMS listing the individuals who can access the CMS data housed at Yale and will also inform CMS when an individual member's participation in research projects is terminated, voluntarily or involuntarily.

4.4. Describe your organization's policies and procedures to ensure original data files are not used following the completion of the project.
The CMS data files are subject to the policies and procedures regarding protected health information (PHI). Yale University has an extensive set of policies for the handling, viewing,

storing, etc. protected health information (PHI) in electronic and paper formats. The HIPAA policies are listed in response to question 7.1.

The PI is responsible for notifying OISPC and the Windows Systems Team (via a ticketing system) when the research project has terminated and the server housing CMS data needs to be decommissioned. Decommissioning procedures will follow the University's Media Control Policy 1609.The following policies and procedures cover all organizational units of Yale University and apply to media in any format that contains confidential information.

- 1609 Media Control Policy and policy sections;
    - 1609.1 General guidelines for media containing confidential information
    - 1609.2 Disposal of media containing confidential information
    - 1609.3 Disposal of media containing confidential information
    - 1609 PR.01 Disposal of Media Containing Confidential or Protected Health Information

Disposal of electronic media containing electronic Protected Health Information is managed by Yale data disposal vendors. Requests for disposal are completed using a Universal Waste Disposal request located on the Yale Website located at http://ehs.yale.edu/universal-waste.

Media must be turned over to Yale's electronic media disposal vendor for destruction at the termination of the study. The vendor uses industry standard methods to dispose of electronic media devices for the University and provides certificates of destruction at the end of the destruction process for hard drives and computer systems.