FINAL REPORT AND RECOMMENDATIONS OF THE DATA PRIVACY AND SECURITY SUBCOMMITTEE OF THE APCD ADVISORY GROUP

August 8, 2019

Report prepared for:
Connecticut APCD Advisory Group

Prepared by:

Dawn Bonder, JD, ***CedarBridge Group***
Michael Matthews, ***CedarBridge Group***

CedarBridge Group LLC
515 NW Saltzman Rd. #661
Portland, OR 97229
www.cedarbridgegroup.com

CEDARBRIDGE GROUP

Table of Contents

Acknowledgements

On behalf of the State of Connecticut, the Executive Director of the Office of Health Strategy and the Health Information Technology Officer express their sincerest gratitude to all those who served on the Data Privacy and Security Subcommittee, as well as those who participated in the work of the group. A strong data privacy and data release policy will provide a critical foundation for the continued success of the All-Payer Claims Database (APCD) as the Office of Health Strategy assumes administrative authority. Your insights, perspectives, and wisdom were invaluable in the development of the policy and recommendations and are a testament of your desire to protect the privacy and confidentiality of individual health data and your commitment to helping improve the health and well-being of the citizens of Connecticut.

Executive Summary and Overview of Recommendations

The Connecticut All-Payer Claims Database (APCD) was created in 2012 by Public Act 12-166. With the passage of Public Act 13-247, the Connecticut General Assembly granted the state's health insurance exchange, Access Health CT (the Exchange), administrative and operational authority over the APCD. Public Act 17-2, as amended by Public Act 18-91, transferred administrative authority from the Exchange to the Office of Health Strategy (OHS). Prior to this transfer, APCD data privacy and security, as well as data release, were governed by the APCD Privacy Policy and Procedure, approved by the Exchange's Board of Directors on February 18, 2016 (APCD Exchange Policy). This shift in authority from the Exchange to OHS necessitated a revised policy.

In November 2018, the APCD Advisory Group re-convened its Data Privacy and Security (DPS) Subcommittee and tasked them with developing a revised policy to address the changes mandated by PA 17-2, as amended by PA 18-91. The DPS Subcommittee's revised policy and recommendations were prepared over the course of its seven meetings from April through July of 2019. The revisions were presented to the APCD Advisory Group on August 8, 2019.

The APCD Exchange Policy provided the DPS Subcommittee a solid foundation from which to begin. Working from that Policy, the DPS Subcommittee updated roles, responsibilities, and definitions to reflect the changes necessary to align with PA 17-2, as amended by PA 18-91. Specifically, the revisions defined the roles and responsibilities of the Executive Director and the Health Information Technology Officer (HITO) of the Office of Health Strategy (OHS), as well as the process by which OHS personnel will interact with and support the Data Release Committee and data release process.

The DPS Subcommittee noted that the APCD Exchange Policy detailed processes and procedures that may have been necessary when the Exchange had administrative authority, but were better-suited as processes and procedures overseen by OHS personnel now that administrative authority has moved to OHS. The DPS Subcommittee identified processes and procedures within the APCD Exchange Policy to be moved to OHS processes and procedures, removed them from the APCD Exchange Policy, and established recommendations for the requirements and methods for maintaining and revising these processes and procedures. These changes are presented as recommendations to the APCD Advisory Group; once accepted and approved, OHS will work to detail the processes and procedures within its governance.

As part of the DPS Subcommittee's work to revise the APCD Exchange Policy pursuant to PA 17-2, as amended by PA 18-91, with support and facilitation from CedarBridge Group, the DPS Subcommittee reviewed other states' policies and procedures to glean best practices and analyze examples of how they are meeting APCD legislative requirements. The DPS Subcommittee also reviewed the extent to which data is released pursuant to other states' governing laws and the degree of transparency of the release process.

This *Final Report and Recommendations of the DPS Subcommittee* represents the conclusion of its work. However, the Subcommittee foresees continued discussion on the type of data and the extent of the Data Release Committee's authority to respond to requests for data from the APCD in order to meet legislative mandates and to achieve sustainability for the APCD.

Project Structure and Process

Public Act No. 17-2[1], was passed during a special session in June 2017, and was further amended by Public Act No. 18-91[2] in May 2018, establishing OHS and the following responsibilities:

(1) Developing and implementing a comprehensive and cohesive health care vision for the state, including, but not limited to, a coordinated state health care cost containment strategy;
(2) Promoting effective health planning and the provision of quality health care in the state in a manner that ensures access for all state residents to cost-effective health care services, avoids the duplication of such services, and improves the availability of financial stability of such services throughout the state;
(3) Directing and overseeing the State Innovation Model (SIM) Initiative and related successor initiatives;
(4) (A) Coordinating the state's health information technology initiatives, (B) seeking funding for and overseeing the planning, implementation and development of policies and procedures for the administration of the all-payer claims database (APCD) program, (C) establishing and maintain a consumer health information Internet web site, and (D) designating an unclassified individual from the office to perform the duties of a health information technology officer (HITO);
(5) Directing and overseeing the Health Systems Planning Unit established under Section 19a-612, and all of its duties and responsibilities as set forth in chapter 368z; and
(6) Convening forums and meetings with state government and external stakeholders, including, but not limited to, the Connecticut Health Insurance Exchange, to discuss health care issues designed to develop effective health care cost and quality strategies.

The APCD Advisory Group charged its Data Privacy and Security (DPS) Subcommittee with responsibility to review and revise the APCD Privacy Policy and Procedure, approved by the Exchange Board of Directors on February 18, 2016 (APCD Exchange Policy) to ensure the policy aligns with the transfer of administrative authority from the Exchange to OHS.

Data Privacy and Security Subcommittee Charge

The DPS Subcommittee was specifically charged with the following goals:

- Review APCD privacy, security, and data release policy practices from other states;
- Review current and anticipated concerns from data recipients, OHS staff,and others;
- Review and revise existing APCD policies to reflect the changes necessitated by Public Act 17-2 as amended by Public Act 18-91; and
- Present recommendations to the APCD Advisory Group for review and affirmation.

By addressing the above goals, the DPS Subcommittee will present an updated policy that reflects the current legislation, as well as the mission and requirements of OHS.

[1] https://www.cga.ct.gov/2017/act/pa/pdf/2017PA-00002-R00SB-01502SS1-PA.pdf
[2] https://www.cga.ct.gov/2018/act/pa/pdf/2018PA-00091-R00HB-05290-PA.pdf

DPS Subcommittee Members

The DPS Subcommittee was reactivated by the APCD Advisory Group. The members of the DPS Subcomittee provided subject matter expertise and stakeholder perspective, as well as institutional knowledge from their experience guiding the development of the APCD Exchange Policy approved in 2016.

Table 1: DPS Subcommittee Members

Name	Affiliation
Dr. Robert Scalatter, Chair	RES Health Strategies / Access Health CT Board Member
Ted Doolittle	Office of the Healthcare Advocate
Patricia Checko, DrPH	Chair, APCD Data Release Committee
Matthew Katz	Connecticut State Medical Society
Joshua Wojcik	Office of the State Comptroller
Jean Rexford	Connecticut Center for Patient Safety
James Iacobellis	Connecticut Hospital Association
Bernie Inskeep	United Health Group
Krista Cattanach	Aetna
Dr. Victor Villagra	University of Connecticut Health, Health Disparities Institute

DPS Subcommittee Process

The DPS Subcommittee's work occurred over seven meetings from April through July of 2019. The first three meetings provided Subcommittee members with background information and helpful context to establish a common understanding of goals, objectives, terminology, and relevant information. During these meetings, CedarBridge Group led Subcommittee members through a review of the privacy, security, and data release practices from 14 states and two national organizations supporting APCDs nationwide. The balance of the Subcommittee's meetings were devoted to crafting an updated policy that would align with legislative provisions and OHS' mission and requirements.

Table 2: DPS Subcommittee Meeting Schedule

Meeting Goal and Focus	Meeting Materials
Meeting #1 (April 26, 9am – 10am) **Kick-off and Orientation** • **Review and discuss project charter** • **Discuss proposed process/workplan for achieving desired outcomes** • **Orientation on Environmental Scan and current policies and procedures for data privacy / release**	• Existing data privacy policies and procedures • Environmental Scan of other APCD initiatives
Meeting #2 (May 3, 9am – 10am) **Consider Current State of Data Privacy Policies** • **Evaluate current APCD data privacy policies** • **Consider new APCD policies to enhance program's effectiveness and efficiency**	• Draft decision criteria • Evaluation matrix
Meeting #3 (May 17, 9am – 10am) **Consider Current Data Release Practices** • **Evaluate current data release policies and procedures** • **Consider new policies/procedures to enhance effectiveness and efficiency** • **Examine potential for APCD data to support approved use cases**	• Existing data release policies and procedures • Application summary
Meeting #4 (May 31, 9am – 10:30 am) **Review Privacy Policy & Recommendations**	• Draft recommendations
Meeting #5 (June 14, 9am – 10:30 am) **Review Privacy Policy & Recommendations**	• Draft recommendations
Meeting #6 (June 28, 9am – 10:30 am) **Review Privacy Policy & Recommendations**	• Draft recommendations
Meeting #7 (July 12, 9am – 10am) **Finalize Recommendations**	• Draft recommendations

Background

Environmental Scan

CedarBridge Group conducted an environmental scan, which included online research and key informant interviews across 14 states with operational APCDs. The scan looked at states with at least as much APCD operational experience as Connecticut, with a particular focus on states with more years of APCD operational experience than Connecticut. At the request of the DPS Subcommittee, more in-depth research was conducted among the neighboring states of New York, Massachusetts, Rhonde Island, and Vermont. Representatives of two national organizations, the APCD Council and the National Association of Health Data Organizations (NAHDO), were also interviewed.

The following APCD characteristics were assessed for each state:

- Treatment of Protected Health Information (PHI)
- Data Release Governance
- Data Release Process
- Transparency of Data Request/Release
- Publication of Security Measures
- Consumer On-line Access to Data
- Treatment of Cost (Pricing) Data

Treatment of PHI – The APCD Exchange Policy used the Health Insurance Portability and Accountability Act (HIPAA) compliance as the standard for treatment of PHI, as did 37% of the states surveyed. Approximately 30% of the states used a more rigorous process requiring an Institutional Review Board (IRB) review or approval of a privacy board. The balance did not store or did not release PHI. The environmental scan indicated a state's ability to collect, store, and release PHI increases the value of an APCD program; it also increases the ability of an APCD program to collect fees for releasing data to requesters for approved uses. States that do not store PHI are not able to integrate claims data with data from other sources, impacting the overall value of the APCD program.

Data Release Governance – The APCD Exchange Policy authorized the Data Release Committee to approve a data release pursuant to a data release request. This was consistent with 20% of the states surveyed. 44% of states surveyed used a process involving multiple committees, depending upon the type of data being requested. Overall, governance of data releases by APCD programs vary widely, depending on the type and complexity of a data request. Some states include stakeholders in the development of data release policies and/or in evaluating data requests by the APCD program. Additionally, some states have begun to include IRB approval as a requirement for APCD programs to release PHI to data requesters.

Data Release Process – The APCD Exchange Policy detailed a very specific data release process that has been effectively guiding the Data Release Committee since its inception. The surveyed states employed a wide variety of processes for evaluating and adjudicating data requests, with no clear model emerging. Trends and observations from the environmental scan show some states moving to streamline processes with online forms and pre-approved data sets for common purposes; some states implementing iterative processes for

data requesters to discuss data needs with APCD staff before making a data request to better understand availability of data and potential limitations, feasibility, and cost; and increasingly detailed data use agreements and required data management plans for data requesters.

Transparency of Data Request/Release – The APCD Exchange Policy required publication of a data request and the disposition of the request on the APCD website. This is consistent with 31% of the states surveyed. However, 56% of states surveyed have no provision for releasing information regarding a data request or release, and 13% of the states surveyed require a public comment period after the notice of the data request is published. States are trending toward providing more transparency around data requests and releases, with interviewees noting that greater transparency has reduced the frequency of challenging requests. States allowing public comments in advance of approving data requests noted that most comments come from healthcare organizations (payors or providers); few comments are from consumers.

Publication of Security Measures – the APCD Exchange Policy cites compliance with HIPAA and/or HITECH, which is consistent with 19% of the states surveyed. 50% of states surveyed had policies that were silent or had a minimal description of security measures. 31% had robust security measures detailed within their APCD policies. States are trending toward less specificity in their published materials about security measures employed by APCD programs; most cite adherence to industry standards and/or regulations. This trend cuts across industries and is not limited to APCD programs or healthcare data systems.

Consumer Online Access to Data – Connecticut currently provides no consumer online access to data, consistent with 25% of states surveyed. 25% of states surveyed provide a library of pre-prepared reports, with the ability to sort and filter. 19% provide public use files, and 31% provide interactive, online tools. Some states are providing interactive online tools for consumers to assess the cost and quality of care offered by providers for specific procedures; these tools vary in ease of use and awareness of their capabilities by consumers. Some states have found that by providing prepared reports and a library of papers, data requests are reduced; however, this could have an unintended consequence for program sustainability by reducing the collection of fees.

Treatment of Cost and Pricing Data – States varied widely on how they made cost and pricing data available to consumers, ranging from no availability to robust, interactive, online tools. While the trend appears to be moving toward disclosing cost/pricing data to consumers, efforts vary. Best efforts (CO, ME, NH, WA) offer robust data (cost and quality) on consumer-friendly, interactive websites that provide information that can be used to make healthcare choices based upon cost and quality for specific health-related procedures. States surveyed indicated that, over time, healthcare organizations become more accepting of publishing price data for specific procedures by an APCD program. This is likely a result of building trust and of shared recognition of the value of the information. Those states releasing pricing data to the public are doing so in a highly curated way to address payor/provider concerns, and also to help ensure the data is easy to understand and unlikely to be misconstrued by consumers.

The environmental scan highlighted the need for states to be cognizant of the levels of stakeholder trust, confidence, and commitment to an APCD program. Trust of stakeholders is essential in order to find consensus positions on data collection and availability for a variety of purposes, especially with respect to:

- APCD data quality
- Accuracy of data reports from APCD program
- Processes used to develop policies and procedures for the APCD program
- Application of and adherence to policies and procedures by the APCD program
- Fairness of APCD data availability and data use policies and procedures

As stakeholder trust and confidence in an APCD program builds, new opportunities for expanding the use of APCD data can be considered. Moreover, as additional uses of APCD data are accepted by stakeholders, the data's value will be more apparent, and support for funding of an APCD program will increase.

Review of Current and Anticipated Concerns

To date, the Data Release Committee has received 15 applications. Twelve have been approved, one has been denied, one is awaiting Data Release Committee review, and one has been submitted to the APCD for release of data.

The DPS Subcommittee reviewed the APCD Exchange Policy, which currently governs privacy and security and data release for the APCD. The process has evolved over time to a more-interactive, iterative process that includes conversations with data requesters prior to review of an application. It is the intent of the Data Release Committee to continue to evolve this process with OHS personnel to improve and streamline the data-request application process, adjudication of the request, and release of APCD data.

During the review process, it was discovered that publication of data requests and releases were not occurring pursuant to the APCD Exchange Policy, and it was noted that OHS will need to ensure these disclosures are made in the future.

The DPS Subcommittee discussed the APCD Exchange Policy's detailed processes and procedures, and noted that it may be more efficient to move some of them from the policy to OHS processes and procedures in order to provide more flexibility and alignment with OHS' mission and process.

It was also noted that the APCD Advisory Group does not have representation from the Data Release Committee, which is a concern for the Data Release Committee members.

DPS Subcommittee Recommendations

Recommendation 1: Purpose of Policy

The DPS Subcommittee recommended broadening the Purpose of Policy section to include an affirmation of intent to protect the privacy and confidentiality of individuals, while also acknowledging the value of APCD data. This is intended to encourage the widest view of APCD data release pursuant to statute and privacy and confidentiality considerations.

Recommendation 2: Add, Delete, and Edit All Definitions, Roles, and Responsibilities to Reflect the Changes Necessitated by PA 17-2 as Amended by PA 18-91

The DPS Subcommittee recommended making the appropriate changes to definitions, titles, roles, and responsibilities in order to align the policy with PA 17-2, as amended by PA 18-91. This includes shifting responsibilities from the Exchange to OHS, from the Exchange CEO to the Executive Director of OHS, and from the Executive Director of the APCD to the HITO.

Recommendation 3: Expand the Composition of the Data Release Committeee

The DPS Subcommittee recommended expanding the composition of the Data Release Committee from eight members to nine members in order to include the Medicaid Director (or a designee), and the Department of Mental Health and Addiction Services Commissioner (or a designee). This will provide clarity for requests seeking commercial as well as Medicaid data.

Recommendation 4: Improve Coordination Between the Data Release Committee and the APCD Advisory Group

The DPS Subcommittee recommended adding the Chair of the Data Release Committee as an APCD Advisory Group member in order to improve coordination and communication between these bodies.

Recommendation 5: The APCD Advisory Group Shall Perform a Review and Evaluation of the Performance of the Data Release Committee

The DPS Subcommittee recommended instituting a review and evaluation of the Data Release Committee's performance by the APCD Advisory Group to ensure both compliance with the policy and continuous process improvement.

Recommendation 6: Move Processes and Procedures From Policy to OHS Oversight

The DPS Subcommittee noted the APCD Exchange Policy included detailed processes and procedures that were necessary for appropriate governance when the Exchange had administrative and operational authority for the APCD. With the shift of administrative authority to OHS, and the complex and lengthy regulatory process required to change policies governed by an agency, the DPS Subcommittee identified processes and procedures that would be better-governed by an agency. These were classified as either internal procedures – those maintained by the HITO that govern the activities necessary for OHS to complete the day-to-day processes required to implement the policy – or external procedures -- those maintained by the HITO that govern the OHS processes related to the ability of the Data Release Committee to review and act on Data Release Applications. Internal procedures may be changed by the HITO with notice to the Data Release Committee, and shall be reviewed every two years to ensure operational effectiveness and process improvement; external procedures require approval of the APCD Advisory Group. A list of the internal and external procedures is provided in the appendix to this report.

Recommendation 7: Further Discussion by the APCD Advisory Group

The DPS Subcommittee recommended the APCD Advisory Group further discuss expansion of the types of APCD data available for release, release of APCD data to national consortiums, and the DPS Subcommittee charge going forward.

Closing Thoughts

Connecticut's APCD has been evolving and fine-tuning its administration and operation since its inception. The shift of administrative authority to the OHS should allow for more streamlined and better-coordinated administration under the oversight of the HITO. The APCD is poised to continue building stakeholder trust with respect to APCD data quality, accuracy of data reports from the APCD program, processes used to develop policies and procedures for the APCD program, application of and adherence to policies and procedures by the APCD program, and fairness of APCD data availability and data use policies and procedures. As trust increases, new opportunities for expanding the use of APCD data can be considered. As stakeholders accept additional uses of APCD data, their value will be more apparent and, as a result, support for funding of an APCD program will increase. In the long term, the value of APCD data will help support a sustainability model for the APCD.

Appendix

Federal and State Legislation Reviewed

Federal Laws:

- Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, Stat. 1936. enacted August 21, 1996
- Privacy Act of 1974, 5 U.S.C. § 552a
- Federal Information Security Management Act, 44 U.S.C. § 3541
- Confidentiality of Substance Use Disorder Patient Records, 42 U.S.C. § 290dd-2; 42 C.F.R. Part 2
- Other requirements relating to uses and disclosures of protected health information, 45 CFR § 164.514

Connecticut Statutes:

- APCD – § 38a-1091 of the 2018 supplement of the general statutes, as amended by PA 18-91
- Establishment of the Office of Health Strategy and associated responsibilities, C.G.S § 19a-754a, as amended by PA 18-91
- Establishment of All-Payer Claims Database Program and associated OHS responsibilities, C.G.S § 19a-755a, as amended by PA 18-91
- Establishment of State-wide Health Information Technology Advisory Council, Advisory Council membership and chairpersons, and establishment of All-Payer Claims Database Advisory Group, C.G.S § 17b-59f, as amended by PA 18-91

Revised APCD Privacy and Security and Data Release Policy

REVISED POLICY V.4 FINAL DRAFT

All-Payer Claims Database (APCD) Privacy Policy and Procedure

1. Purpose of Policy.

   a. APCD Legislative Mandate and History. Public Act 13-247 enabled the Exchange's creation of the Connecticut All-Payer Claims Database ("APCD"). Pursuant to Public Act 13-247, various Data Submitters are required to report healthcare information to the Exchange for inclusion in the APCD. The Act allows the Exchange: (i) to utilize healthcare information collected from Data Submitters to provide healthcare consumers in Connecticut with information concerning the cost and quality of healthcare services that allows such consumers to make more informed healthcare decisions; and (ii) to disclose Data to state agencies, insurers, employers, healthcare providers, consumers, researchers and others for purposes of reviewing such Data as it relates to health care utilization, costs or quality of healthcare services. Public Act 17-2, as amended by Public Act 18-91, transferred administrative authority of the APCD from the Exchange to OHS.

   b. Purpose of the Policy. The purpose of this Policy is to ensure the integrity, security, and appropriate use and disclosure of Data. The policy is intended to provide necessary safeguards to ensure the confidentiality and privacy of individuals, while also acknowledging the value of the Data and benefits from appropriately sharing such Data.

2. Definitions.

   a. "*Act*" means Connecticut General Statutes Sections 38a-1090, 38a-1091, and Public Act 17-2, as amended by 18-91, as amended from time to time.

   b. "*Advisory Group*" shall mean the All-Payer Claims Database Advisory Group established pursuant to the Act.

   c. "*APCD*" means the Connecticut All-Payer Claims Database established by the Act and created and maintained by OHS.

   d. "*APCD Personnel*" means those OHS employees, agents and contractors (other than the contractor responsible for receiving healthcare information from the Data Submitters) whom the HITO permits, in writing, to access Data through the Managed Environment or Vendor.

   e. "*Applicant*" means an individual or organization that requests access to Data by submitting a Data Release Application to the HITO.

f. "*Applicant Related Party*" means any individual or entity under common ownership or control of an Applicant.

g. "*Data*" means De-Identified claim information provided to the APCD by Data Submitters and made available through the Vendor or Managed Environment.

h. "*DPS"* means the Data Privacy and Security Subcommittee of the APCD Advisory Group charged with ensuring the integrity, security, and appropriate use and disclosure of Data.

i. "*Data Release Application*" means the written application and supporting documentation or other materials an Applicant submits to the HITO or the Data Release Committee in connection with a request to access Data.

j. "*Data Release Committee*" means the committee responsible for reviewing and acting on Data Release Applications.

k. "*Data Submitters*" means: (i) those entities and/or organizations required to report healthcare claims information to the APCD pursuant to the Act; and (ii) Connecticut state agencies, hospitals, the United States Census Bureau, governmental payers, such as Medicare and Medicaid, and any other third parties who submit healthcare claims information to the APCD.

l. "*Data Use Agreement*" means the written agreement entered into by and between an Applicant and OHS upon acceptance of the Applicant's Data Release Application by the Data Release Committee, which sets forth the obligations and responsibilities of the Applicant with respect to the use of the Data disclosed to it by OHS.

m. "*De-Identified*" refers to healthcare information from which all eighteen (18) identifiers enumerated at 45 C.F.R. § 164.514(b)(2) have been removed.

n. "*Exchange*" means The Connecticut Health Insurance Exchange d/b/a "Access Health CT".

o. "*Executive Director"* means the Executive Director of the OHS.

p. *"External Procedures*" mean the set of procedures maintained by the HITO that govern the OHS processes related to the ability of the DRC to review and act on Data Release Applications.

q. "*HIPAA*" means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, each as amended from time to time.

r. "*HITO*" means Health Information Technology Officer for the Office of Health Strategy.

s. "*Internal Procedures"* mean the set of procedures maintained by the HITO that govern the activities necessary for OHS to complete the day-to-day processes required to implement this Policy.

t. "*Limited Data Set*" means healthcare information from which all sixteen (16) identifiers enumerated 45 C.F.R. § 164.514(e)(2) have been removed.

u. "*Managed Environment*" means the computer interface by which the OHS accesses Data.

v. "*OHS"* means the Office of Health Strategy.

w. "*Project"* means the purpose or program for which Data is disclosed to a Recipient.

x. "*Recipient"* means an Applicant whose Data Release Application has been approved by the Data Release Committee and which has received Data from the APCD.

y. "*Recipient Third Party*" means an employee, agent or contractor of a Recipient or any entity or organization to which the Recipient has redisclosed or made available Data.

z. "*State*" means the state of Connecticut.

aa. "*Work Product*" means every invention, modification, discovery, design, development, customization, configuration, improvement, process, work of authorship, documentation, formulae, datum, code, technique, reporting logic, know how, secret, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registerable under copyright or similar statutes or subject to analogous protection) that is made, conceived, discovered, or reduced to practice by a Recipient or Recipient Third Party.

bb. "*Vendor*" means the entity or organization engaged by OHS to provide data management or maintenance services with respect to the APCD.

3. Health Information Technology Officer.

a. The Health Information Technology Officer (HITO) shall have general oversight responsibility for the privacy, security, and access to Data by potential Recipients. The HITO's authority is subject to all state statutes, rules, and regulations, as well as all OHS policies. In all instances, the HITO may delegate functions or responsibilities to other properly qualified OHS employees, agents or contractors acting in accordance with this Policy.

b. The HITO shall maintain a list of each member of the Data

Release Committee and his or her professional affiliation and shall make

such list available to the public.

c. The HITO shall maintain a set of Internal Procedures and External Procedures for the execution of its oversight under this Policy.

i. Internal Procedures will govern the activities necessary for OHS to complete the day-to-day processes required to implement this Policy. The HITO shall have authority to make changes to the Internal Procedures at his or her discretion, provided the DPS is notified of changes.

ii. Internal Procedures shall be reviewed by the DPS every two years to ensure operational effectiveness and process improvement.

iii. External Procedures will govern the OHS processes overseen by the HITO related to the ability of the DRC to review and act on Data Release Applications. Changes to the External Procedures will require the approval of the APCD Advisory Group.

4. Data Release Committee.

a. Purpose and Mission. The purpose of the Data Release Committee shall be to: (i) review, approve and deny Data Release Applications (in accordance with this policy and established procedures) submitted by Applicants for the release of Data; and (ii) provide support to the HITO during the receipt and review of Data Release Applications.

b. Governance.

i. Committee Members. The Data Release Committee shall consist of not less than nine (9) members and shall be composed of at least the following: (i) The Medicaid Director or his/her designee; (ii) The Department of Mental Health and Addiction Services (DMHAS) Commissioner or his/her designee; (iii) the HITO; (iv) an individual with a professional or academic research background involving public health matters; (v) a representative from the health insurance industry; (vi) an attorney with experience in health care, data privacy or research matters; (vii) a healthcare professional, such as a physician, nurse, social worker or psychologist; (viii) an individual with experience in hospital administration, analytics or research; and (ix) a consumer representative (each a "Member" and collectively the "Members").

ii. Appointment and Removal. Members shall be appointed by and serve at the pleasure of the Executive Director. When appointing a Member, the Executive Director shall consider nominations from the HITO and Chair of the Data Release

Committee. The Executive Director may remove and replace Members at any time in his/her discretion.

iii. Voting Rights. Each Member shall have one vote.

iv. Terms. There shall be no term limits with respect to Members.

v. Chairperson. The Executive Director shall designate a Member of the Data Release Committee to act as chairperson of the Data Release Committee ("Committee Chair") and may designate one or more vice chairs to act only in the absence of the Committee Chair.

The Committee Chair (or Vice Chair, in the Committee Chair's absence) shall preside at meetings of the Data Release Committee.

c. Meetings.

i. The Data Release Committee shall meet at least quarterly, or more frequently as circumstances dictate, in accordance with a schedule set by the HITO.

ii. All meetings of the Data Release Committee shall be open to the public. Deliberation of confidential information shall be conducted in executive session in accordance with applicable law.

d. Voting.

i. Voting/Quorum. A majority of the Members of the Data Release Committee shall constitute a quorum for the transaction of business, and the vote of a majority of Members present shall be required for the Data Release Committee to take formal action.

ii. Recusals/Conflicts of Interest. Each Member shall be free from any relationships or conflicts of interest with respect to an Applicant that may impair, or appear to impair, the Member's ability to make independent judgments. In the event of any such relationship or conflict of interest, the Member shall disclose such conflict and if necessary, recuse him/herself from any review, discussion or deliberation involving or relating to the Applicant's Data Release Application.

e. Delegation. The Members shall have no right to delegate any functions or responsibilities hereunder to any third-party individual or entity.

f. Coordination. The Chair of the DRC shall be a standing member of the Advisory Group.

5. Use of Data by OHS.

a. Access to Data by APCD Personnel.

i. The APCD Personnel shall be the only individuals permitted to access Data through the Vendor or Managed Environment.

ii. All APCD Personnel shall be credentialed in accordance with applicable OHS policies and procedures prior to being granted access to the Data through the Vendor or Managed Environment. Access to the Data through the Vendor or Managed Environment shall be subject to the applicable access authentication and audit report requirements of OHS's security program and policies, including but not limited to the use of dual-factor authentication.

b. Use of the Managed Environment and Data

i. APCD Personnel may access Data through the Managed Environment or Vendor only (i) to review and analyze such Data for purposes of fulfilling OHS' mandate under the Act, including but not limited to the preparation of consumer and public facing reports and analyses, or (ii) for OHS internal business administration or operations. Any access of Data by APCD Personnel inconsistent with this Policy will be subject to OHS personnel policies.

ii. All Data accessed through the Managed Environment or Vendor by APCD Personnel shall be De-Identified. Notwithstanding, the HITO may, in his or her discretion, permit designated APCD Personnel to access a Limited Data Set from the Managed Environment or Vendor. APCD Personnel granted access to a

Limited Data Set by the HITO shall keep such Limited Data Set strictly confidential and shall not disclose, or provide access to, the Limited Data Set to any other individual, either internal or external to OHS without the prior written consent of the HITO.

iii. APCD Personnel may not access Data through the Managed Environment or Vendor, or otherwise use or disclose such Data, for (i) any private or illegal purpose, or (ii) any purpose inconsistent with the Act or this Policy.

iv. When accessing and using the Managed Environment or obtaining Data through the Vendor, APCD Personnel shall: (i) never install any software, application or code in the Managed Environment, unless specific written approval has been provided by the HITO; (ii) never link external data with Data from Managed Environment or the Vendor without prior written approval from the HITO; and (iii) not re-identify, or attempt to reidentify, Data.

v. OHS shall maintain: (i) copies of the Managed Environment and Vendor output and make such information available for the purpose of conducting security audits; and (ii) Managed Environment and Vendor access logs.

c. Disclosure of Data by APCD Personnel.

i. APCD Personnel may not disclose any Data accessed through the Managed Environment or Vendor except: (i) as explicitly permitted by this Policy, including but not limited to disclosure after approval of a Data Release Application by the Data Release Committee; (ii) with the written consent of the HITO and after the execution of a written confidentiality agreement between OHS and the approved recipient, when such disclosure is reasonably necessary for the operations of OHS or fulfillment of the purpose of the Act; or (iii) as required by state or federal law, regulation or process. Any disclosure of Data by APCD Personnel inconsistent with this Policy will be subject to OHS personnel policies.

ii. Any third-party vendor engaged by OHS to maintain, use or disclose the Data, including the Vendor, shall comply with all applicable OHS policies and procedures and shall implement and maintain technical, physical, and administrative standards sufficient to protect and ensure the privacy and security of the Data, including but not limited to: (i) the specifications and requirements set forth in applicable State and federal law; (ii) industry standards and best practices regarding the maintenance and security of healthcare data, and (iii) the third-party vendor's privacy and security policies, procedures and protocols.

d. Safeguarding Data in the OHS' Possession.

i. All Data shall be maintained in accordance with applicable OHS security policies, protocols and procedures.

e. Disposal of Data in OHS' Possession.

i. All Data maintained on electronic media shall be sanitized in accordance with OHS policy and procedure.

ii. All Data maintained in paper format shall be shredded, pulverized or otherwise destroyed in a manner that prevents re-identification or reassemblage of the Data.

6. Data Release Application Process.

a. Data Release Application. OHS shall develop and maintain a Data Release Application. The HITO shall retain the right, in his or her sole discretion, to modify the Data Release Application for

particular Applicants or Projects; provided such modification is consistent with this Policy and applicable law.

b. Submission. An Applicant must submit a complete Data Release Application to OHS and be willing to be interviewed by the Data Release Committee.

c. Data Release Application Processing Fees. The HITO shall collect a processing fee for each Data Release Application received. The HITO shall create and publish a fee schedule for such processing fees.

d. Data Release Application Review Process.

i. Role of HITO.

1. Upon receipt of a Data Release Application for an Applicant, the HITO shall, pursuant to OHS procedures, review and determine if the Data Release Application is complete and ready to be submitted to the Data Release Committee for review.

2. HITO shall ensure the following information is posted to the APCD public-facing website once a Data Release Application is received: (i) Applicant name and contact information; and (ii) description and purpose of Project.

ii. Review by Data Release Committee.

1. Upon receipt of a Data Release Application from the HITO, the Data Release Committee shall review the Data Release Application in a timely manner, as specified by OHS procedures. Such review shall include, but not be limited to, the following:

a. Determine whether the Data Release Application is consistent with the objectives of the APCD as set forth in the Act;

b. Review whether the Applicant would be able to reidentify the Data provided;

c. Determine the adequacy of the Applicant's privacy and security infrastructure and safeguards;

d. Any other factor or consideration deemed by the HITO or Data Release Committee to be relevant to the Data Release Application or Project; and

e. If the Data Release Application is from a researcher or is otherwise for research purposes, determine whether the research methodology is consistent with established norms and the Data Release Application sets forth a sound research design.

2. Right to request additional information. The Data Release Committee shall have the right to direct the HITO to request additional information, seek clarification from the Applicant, or request a meeting with the Applicant.

3. Support by HITO and OHS. The Data Release Committee may seek assistance, guidance and technical advice from the HITO or the staff of OHS at any time during its review and consideration of a Data Release Application. The Data Release Committee may also obtain assistance, guidance and technical advice from third parties including but not limited to dataset design professionals, clinicians, health insurance experts, privacy experts, attorneys and regulatory authorities; provided it does not delegate its responsibilities hereunder.

4. Decisions. (i) Upon completion of its review and consideration of a Data Release Application, the Data Release Committee may issue one of the following three decisions:

a. Approval. Approval is to be granted when the Data Release Committee determines, in its sole discretion, that the Data Release Application satisfies each of the requirements and criteria outlined in this Policy and the Data Release Application.

b. Conditional Approval. Conditional approval is to be granted when the Data Release Committee requires additional information from, or actions by, the Applicant in order to address outstanding issues, and the Data Release Committee determines, in its sole discretion, that such additional information or actions will (i) adequately address and satisfy any concerns of the Data Release Committee; and (ii) permit the Data Release Committee to determine, in its sole discretion, that the Data Release Application satisfies each of the requirements and criteria outlined in this Policy and the Data Release Application.

c. Denial. Denial is to be issued when the Data Release

Committee determines, in its sole discretion, that the Data Release Application fails to satisfy one or more requirements or criteria outlined in the Act or this Policy.

iii. Veto Authority. The Executive Director reserves the right to veto any decision of the Data Release Committee if he/she determines, in his/her sole discretion, that the Data Release Application fails to satisfy one or more requirements or criteria outlined in the Act or this Policy. Upon the exercise of this right, the Executive Director shall provide the rationale underlying the veto to the Data Release Committee and the Applicant.

iv. No Right of Appeal. An Applicant shall have no right to appeal a decision on a Data Release Application made by the Executive Director, HITO, or the Data Release Committee.

v. Opportunity for Resubmission of Data Release Application. An Applicant which has submitted a Data Release Application that is subsequently denied may re-submit the Data Release Application for re-consideration. The HITO also has the discretion to deny consideration of a new Data Release Application if upon preliminary review by the HITO, the Data Release Application has not materially changed.

7. Release of Data Pursuant to Approved Data Release Applications.

a. Data Use Agreement.

i. The HITO, in consultation with OHS and the Data Release Committee, shall develop a template Data Use Agreement. The Data Use Agreement shall, at a minimum, require the Recipient to: (i) ensure that Data will be used and re-disclosed only for purposes of the Project; (ii) adequately safeguard the privacy and security of the Data; (iii) grant OHS and its designated agents access to the Recipient's premises for purposes of determining compliance with the Data Use Agreement; (iv) agree to all policies and procedures of OHS applicable to the APCD, including those addressing cell suppression and this Policy, as applicable; (v) not re-identify, or seek to re-identify, any Data; (vi) if applicable, provide the HITO an advance copy of any research or analysis results, publications or manuscripts to determine whether or not the privacy or security of the Data has been compromised in any way; (vii) assign a person to be responsible for the privacy and security of the Data while in Recipient's possession or control; (viii) maintain logs of all individuals and entities who access, use or receive Data, and make such logs available to the HITO upon request; (ix) immediately report any unauthorized use or disclosure of Data; (x) not use Data for any unlawful purpose; (xi) require Recipient Related Parties to agree, in writing, to the requirements, terms and conditions of the Data Use Agreement; (xii) notify OHS within thirty (30) calendar days of completion of the Project and either return or destroy all Data in accordance with this Policy; (xiii) during all times during which the Data is in the possession or control of the Recipient or a Recipient Related Party, maintain internal written logs recording (a) the date of each use or

disclosure of the Data, (b) the identity of each user or recipient of the Data, and (c) the purpose of such use or disclosure; and (xiv) to the extent permitted by law and principles of sovereign immunity, indemnify, defend and hold OHS and the State harmless from any and all claims, losses, liabilities, damages, judgments, fee, expenses, awards, penalties and costs relating to or arising from the use or disclosure of the Data, or the violation of the Data Use Agreement or any applicable law, by the Recipient or Recipient Related Party. In the event that the Recipient is a State agency, and such indemnification is impermissible under State law, such agency shall be required to assume responsibility for any remediation necessary to protect individuals subject to a Data breach that results in re-identification of the subject of the Data.

ii. Upon approval or conditional approval of a Data Release Application in accordance with Section 6(d)(4) of this Policy, the

HITO shall provide a Data Use Agreement to the Applicant for review and execution. The Data Use Agreement provided to the Applicant shall be non-negotiable.

iii. In the event the HITO determines that the Recipient has violated any term or condition of the Data Use Agreement, OHS may do any of the following in its sole discretion: (i) immediately cancel the Data Use Agreement; (ii) require the immediate return or destruction of the Data; (iii) if access to the Data is provided via the Enclave Model, immediately terminate the Recipient's access to the Data; (iv) deny the Recipient access to any further Data from the APCD; and/or (v) institute legal proceedings against the Recipient.

iv. In the event an Applicant or an Applicant Related Party has, in the sole discretion of the HITO or Data Release Committee, previously violated any term or condition of a Data Use Agreement entered into between OHS and such Applicant or Applicant Related Party, the HITO may deny such Applicant or Applicant Related Party the opportunity to re-submit and existing, or submit a new, Data Release Application.

b. Form/Manner of Access. Upon execution of a Data Use Agreement, OHS shall make Data available to a Recipient. The HITO, in consultation with the Recipient, shall select the manner of access most appropriate for the Recipient and its approved Project and shall ensure that the access is secure.

c. De-Identification. Data released to a Recipient shall not be provided with any key, protocol or map that would allow the Data to be re-identified.

d. Minimum Necessary. OHS shall release only the Data the HITO and/or Data Release Committee, in consultation with the Applicant, determines to be the minimum necessary for the Applicant to conduct the Project.

e. Access Fees. OHS, in its discretion, may charge fees to Recipients for access to Data. In the event such fees are charged, the HITO shall create and publish a schedule of such access fees.

f. Posting of Data Release Application Disposition on APCD Website. HITO shall ensure the disposition of the Data Release Application is posted on the APCD public-facing website.

8. Return or Destruction of Data.

a. Return or Destruction of Data. In the event the Recipient, or any Recipient Related Party, violates any term or condition of the Data Use Agreement entered into by and between OHS and the Recipient, or at the end of any Project, the HITO may require the Recipient, or any Recipient Related Party, to return to OHS or destroy any or all Data in the Recipient's or the Recipient Related Party's possession or control. The HITO reserves the right, in his or her sole discretion, to require a particular method and/or schedule of return or destruction.

b. Standard of Destruction. All Data maintained on electronic media shall be sanitized in accordance with OHS procedures, utilizing National Institute of Standards and Technology (NIST) requirements. All Data maintained in paper format shall be shredded, pulverized or otherwise destroyed in a manner that prevents re-identification or re-assemblage of the Data.

c. Certification of Return or Destruction. The HITO may require, in his or her sole discretion, the Recipient to certify, in writing, that all Data in the Recipient's possession or control, or in the possession or control of any Recipient Related Party, has been returned to OHS or destroyed in accordance with this Policy and OHS procedure.

9. Ownership of Data and Work Product.

a. Ownership of Data. Neither a Recipient nor a Recipient Related Party shall have any ownership or property rights or interests in the Data received from OHS.

b. Ownership of Work Product. OHS shall not obtain any ownership rights to any Work Product developed or prepared by a Recipient or a Recipient Related Party.

c. Publications. Recipient may publish, otherwise publicly disclose, or submit for publication an article, manuscript, abstract, report, poster, presentation, or other material that includes the results of the use of the Data, as would be reasonably required for purposes of publication in a peer-reviewed scientific journal (such article, manuscript, abstract, report, poster, presentation, or other material, a "Manuscript"), pursuant to OHS policies and procedures.

10. Annual Reporting.

a. The APCD Advisory Group shall perform a review and evaluation, at least annually, of the performance of the Data Release Committee, including reviewing the compliance of the Data Release Committee with this Policy. In addition, the APCD Advisory Group shall review

and reassess, at least annually, the adequacy of this Policy and recommend to the Executive Director any improvements to this Policy that the APCD Advisory Group considers necessary or valuable.

b. The Data Release Committee shall submit a report to the APCD Advisory Group, at least annually, outlining the Data Release Committee's activities, statistics relating to the volume and type of Data Release Applications received, the review and acceptance or rejection of Data Release Applications and the percentage of Data Release Applications that did and did not result in publication. The report shall include any recommendations for improvements to this Policy the Data Release Committee considers necessary or valuable.

11. Conflicts.

a. In the event of any actual or perceived conflict between an OHS policy or procedure and this Policy, this Policy shall control, except as may be necessary to comply with any applicable law or regulation.

b. In the event that any law or regulation is enacted or promulgated that is in any way inconsistent with the terms of this Policy or that interferes with the OHS obligations hereunder, this Policy shall be deemed to be automatically amended to comply with such law or regulation.

12. Confidentiality.

Notwithstanding anything herein to the contrary, OHS and the Data Release Committee shall comply with all applicable laws and regulations regarding confidentiality, including but not limited to the Connecticut Freedom of Information Act set forth at Connecticut General Statutes Sec. 1-200, *et. seq*., as may be amended from time to time.

Summary of Processes and Procedures (Attachment A)

Environmental Scan Results by State (Attachment B)

Red-lined APCD Privacy and Security and Data Release Policy (Attachment C)