

**All-Payer Claims Database (APCD) Data Privacy and Security Subcommittee -  
Special Meeting**

**NOTICE OF SPECIAL MEETING AND AGENDA**

Date: **Friday, May 8, 2015**

Time: **9:00 a.m. to 11:00 a.m.**

Webinar Link: Click here to join online meeting:  
<http://www.mymeetings.com/nc/join.php?sigKey=mymeetings&i=279332022&p=&t=c>

Conference Line: Phone Number: (866) 732-1486  
Participant Code: 777801458#

Location\* Hilton Hartford, Connecticut Ballroom – Salon C  
315 Trumbull Street, Hartford, CT 06103

Directions: <http://www3.hilton.com/en/hotels/connecticut/hilton-hartford-HFDHHEH/maps-directions/index.html>

---

- I. Call to Order and Introductions
- II. Public Comment
- III. Approval of January 8 Meeting Minutes
- IV. Chairperson Update
- V. Presentation of Proposed Policies and Procedures
- VI. Timeline for Approval of Policies and Procedures
- VII. Next Steps
- VIII. Future Meetings
- IX. Adjournment

---

*Webinar details available on page 2.*

*A note regarding attendance:*

*Member attendance by phone and online is agreeable. Members will introduce themselves at beginning of meeting to confirm attendance at the start of the meeting.*

## Webinar Participation Details

---

### I. Conferencing into the meeting:

Phone: (866) 732-1486

Code: 777801458#

### II. Joining the Online Webinar:

1. Click the following link to join the webinar now:

<http://www.mymeetings.com/nc/join.php?sigKey=mymeetings&i=279332022&p=&t=c>

2. Enter any required fields.
3. Indicate that you have read the Privacy Policy.
4. Click on Proceed. You will be placed into the webinar at that time.

---

Webinar Meeting Number: 279332022

Public comment of the agenda is limited to two minutes per person and is not to exceed the first 15 minutes of each meeting. A sign-in sheet will be provided.

---

Access Health CT is pleased to make reasonable accommodations for members of the public who are disabled and wish to attend the meeting. If special arrangements for the meeting are necessary, please notify Christen Orticari at (860) 241-8444. For further information concerning this meeting, please contact Christen Orticari at (860) 241-8444 or [Christen.Orticari@ct.gov](mailto:Christen.Orticari@ct.gov).

---

Meeting materials will become available at: [www.ct.gov/hix](http://www.ct.gov/hix) following each meeting.



APCD Data Privacy and Security Subcommittee Special Meeting  
**Draft Meeting Minutes**

**Date:** Thursday, January 8, 2015  
**Time:** 9:00 a.m. – 11:00 a.m. EST  
**Location:** Hilton Hartford Hotel, Hartford Commons Room

---

**Members Present**

Dr. Robert Scalettar (Chair), Dr. Robert Aseltine (Phone), Demian Fontanella, James Iacobellis, Matthew Katz (phone), Jean Rexford, Shawn Rutchick, Mary Taylor, Joshua Wojcik, Dr. Victor Villagra

**Members Absent**

Phyllis Hyman

**Other Participants**

Dr. Tamim Ahmed, Robert Blundo, Christen Orticari, Joan Feldman, William Roberts

---

**I. Call to Order and Introductions**

Dr. Robert Scalettar called the meeting to order at 9:00 am. Members introduced themselves.

**II. Public Comment**

There was no public comment made at this time.

**III. Approval of November 13, 2014 Meeting Minutes**

Dr. Scalettar asked for a motion to approve the April 1 and June 26, 2014 meeting minutes. Mary Taylor motioned to approve the April 1 and June 26, 2014 meeting minutes. Dr. Victor Villagra seconded. Motion passed.

**IV. Chairperson Update**

Dr. Scalettar gave an update on AHCT's new contract with Onpoint Health Data (OHD) for the provision of APCD data management and analytical services. The partnership was publically announced on November 11 and presented at the APCD Advisory Group Meeting on November 13. He thanked Dr. Tamim Ahmed, Robert Blundo, Matthew Salner, Christen Orticari, and the Attorneys at Shipman and Goodwin, Joan Feldman and William Roberts, for their role in completing the contract. At the June 26 meeting, the subcommittee voted for staff to build a proposed 'strawman' data governance model, including a proposed strategy for the composition and structure of the Data Release Application (DRA), Data Review and Release Committee (DRRC), and Data Use Agreement (DUA) to guide the development policy and procedure amendments. The goal of the meeting presentation was for members to review, discuss and give feedback on the model.

**V. Proposed Straw Man Model**

**Data Request Application (DRA) Process**

Dr. Ahmed briefed members on aspects of the Policy and Procedures document that necessitated the development of a data governance framework. Then he presented a schematic of the data review and disclosure processes, gave a high-level overview of the role of the data requestor, data release entity, DRRC members and staff.

Dr. Ahmed summarized information that the Data Release Application (DRA) required of an entity requesting data. Dr. Ahmed added that in the event an applicant was denied for a particular data request, and not on the basis of prior non-compliance consideration, the applicant had to re-submit a new DRA to be reconsidered by the APCD Administrator,

and DRRC. Ms. Feldman suggested that any non-compliance issues be addressed by building in an indemnification component to the Data Release Application (DRA).

**Data Review and Release Committee (DRRC) composition, structure, tasks and process**

Dr. Ahmed presented the strategy for developing the Data Review and Release Committee (DRRC) composition, structure, tasks and processes. In other states, the DRRC was a standalone committee and membership did not seem to overlap with other workgroups.

Dr. Ahmed explained the tasks that DRRC members were expected to perform and the support that staff contributed to the process from the time an application was submitted to its approval or denial. Then, he presented a preliminary outline of administrative tasks, rules and regulations anticipated throughout the data application review and disclosure process to guide the development of proposed amendments to the Policies and Procedures.

**Discussion:**

- Dr. Victor Villagra recommended that professionals external to the APCD Advisory Group be considered for DRRC membership. Jean Rexford suggested adding Nurse Representative in the DRRC.
- Demian Fontanella added that a quorum was needed for decisions to be made at DRRC. Details regarding quorum requirements needed further consideration.
- Members suggested an honorarium for members in the DRRC. Staff planned to research this issue based on experiences from other APCDs.

**Data Use Agreement (DUA)**

Dr. Ahmed reported content requirements for Data Use Agreement (DUA) composition. For instance, DUA terms contractually required an approved requesting entity to provide logs of all data users, report any unauthorized uses or disclosures of data, and must indemnify, defend, and hold AHA harmless from any and all claims, losses, liabilities, damages, judgments, fees, expenses, awards, penalties and costs in the event of non-compliance.

Ms. Feldman suggested including a provision in the DUA stating that, if a report was published, then AHA had the right to add a content link to the report on the APCD website to showcase hypotheses that were supported by APCD data. Without this provision, an approved requesting entity owned their report results and their publishing rights, and was not required to permit AHA the right to put a link to their report. Then, the copyright would be owned by that journal.

**Discussion:**

- Members asked whether all members on DRRC need to sign off on a DUA.
- Dr. Victor Villagra emphasized that infrastructural security was critical to consider when planning the technical design of the data request and disclosure process and DUA contract. He suggested that an entity approved to receive data be required to provide evidence of infrastructural security to verify that they are technically equipped to securely maintain the information in accordance with required standards.
- Members expressed concern about the data destruction process. Although the proposed DUA content required a certificate of data destruction, members opined that the requirement should include more tangible evidence of data destruction
- Shawn Rutchick pointed out that a different kind of contract was needed for state agencies, since any request from the state of Connecticut, required approval from the Connecticut Attorney General's Office.

**VI. Next Steps**

Mr. Ahmed asked for members to send staff their comments, suggestions, and questions on the content presented during the meeting. On receipt of members' comments, suggestions and questions, they were sent to Ms. Feldman and Mr. Roberts for their consideration when drafting the data governance and disclosure amendments to the APCD Policies and Procedures.

Dr. Scalettar announced that Mary Taylor needed to withdraw from the subcommittee to reduce the frequency of travel required due to her service to multiple other committees. She planned to continue her service as a member of the APCD Advisory Group. Ms. Taylor identified a replacement, Tracey Scraba, Senior Counsel, Aetna Legal and Regulatory Affairs. As one of the legal advisors to Aetna's Data Governance Board, she was well versed in privacy law

and had practical experience in data use and data release cases from the carrier perspective. Dr. Scalettar welcomed Ms. Scraba as a new member of the subcommittee.

**VII. Future Meetings**

Staff sent an email to members with proposed dates in March to schedule the next meeting following adjournment.

**VIII. Adjournment**

**Dr. Scalettar asked for a motion to adjourn the meeting. Demian Fontanella motioned. Ms. Taylor seconded. Motion passed unanimously. Meeting adjourned at 11:00 AM.**

DRAFT

## Access Health CT

### 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 health care information to the Exchange for inclusion in the APCD. The Act allows the Exchange: (i) to utilize Data collected from Data Submitters to provide health care consumers in Connecticut with information concerning the cost and quality of health care services that allows such consumers to make more informed health care decisions; and (ii) to disclose health information data collected by the APCD to state agencies, insurers, employers, health care providers, consumers, researchers and others for purposes of reviewing such data as it relates to health care utilization, costs or quality of health care services.
  - b. Purpose of the Policy. The purpose of this Policy is to ensure the integrity, security and appropriate use of Data collected by the APCD. More specifically, to set forth the process and procedure by which the Exchange will accept, review and evaluate applications from third parties requesting access to the Data collected by the Exchange in a manner consistent with the Act.
2. Definitions.
  - a. "Act" means Connecticut General Statutes Sections 38a-1090 and 38a-1091, 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 the Exchange.
  - d. "Applicant" means an individual or organization that requests access to Data by submitting a Data Release Application to the Executive Director.
  - e. "Applicant Related Party" means any individual or entity under common ownership or control of an Applicant.
  - f. "Board" means the Board of Directors of the Exchange constituted pursuant to Public Act No. 11-53 and the Bylaws of the Exchange.

- g. “*Data*” means claim information, including health information, provided to the APCD by Data Submitters.
- h. “*Data Release Application*” means the written application and supporting documentation or other materials an Applicant submits to the Executive Director or the Data Release and Review Committee in connection with a request to access Data.
- i. “*Data Release and Review Committee*” means a subcommittee of the Board responsible for reviewing and making recommendations to the Executive Director regarding the acceptance or denial of Data Release Applications.
- j. “*Data Submitters*” means: (i) those entities and/or organizations required to report Data 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 Data to the APCD.
- k. “*Data Use Agreement*” means the written agreement entered into by and between an Applicant and the Exchange upon acceptance of the Applicant’s Data Release Application by the Data Release and Review Committee, which sets forth the obligations and responsibilities of the Applicant with respect to the use of the Data disclosed to it by the Exchange.
- l. “*De-Identified*” means Data from which all eighteen (18) identifiers enumerated at 45 C.F.R. § 164.514(b)(2) have been removed.
- m. “*Executive Director*” means the individual appointed by the Exchange to serve as executive director of the APCD.
- n. “*Exchange*” means The Connecticut Health Insurance Exchange d/b/a “Access Health CT”.
- o. “*HIPAA*” means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, each as amended from time to time.
- p. “*Limited Data Set*” means Data from which all sixteen (16) identifiers enumerated 45 C.F.R. § 164.514(e)(2) have been removed.
- q. “*Managed Environment*” means the computer interface by which the Exchange accesses Data.
- r. “*Privacy Officer*” means the individual appointed by the Exchange to have responsibility for the privacy and confidentiality of information maintained by the Exchange.

- s. “*Project*” means the purpose or program for which Data is disclosed to a Recipient.
- t. “*Recipient*” means an Applicant whose Data Release Application has been approved by the Data Release and Review Committee and which has received Data from the APCD.
- u. “*Recipient Third Party*” means an employee, agent or contractor of a Recipient or any entity or organization to which the Recipient has re-disclosed or made available Data.
- v. “*State*” means the state of Connecticut.
- w. “*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.

3. Executive Director.

- a. The Executive Director shall have general oversight responsibility for the privacy, security and access to Data by potential Recipients. In all instances, the Executive Director may delegate functions or responsibilities to other properly qualified Exchange employees, agents or contractors acting in accordance with this Policy.
- b. The Executive Director shall maintain a list of each member of the Data Release and Review Committee and his or her professional affiliation and shall make such list available to the public on the Exchange’s public-facing website. The Executive Director shall revise and update such list as necessary.
- c. The Executive Director shall establish a meeting schedule for the Data Release and Review Committee and communicate that schedule, and any changes thereto, to each member of the Data Release and Review Committee in a timely manner.

4. Data Release and Review Committee.

- a. Purpose and Mission. The purpose of the Data Release and Review Committee shall be to: (i) review, approve and deny Data Release Applications (in accordance with established guidelines) submitted by

Applicants for the release of Data; and (ii) provide support to the Executive Director during the receipt and review of Data Release Applications.

b. Governance.

- i. Committee Members. The Data Release and Review Committee shall consist of not less than eleven (11) members and shall be composed of at least the following: (i) at least two (2) individuals who are not *ex officio* members of the Board; (ii) at least one (1) individual who is an *ex officio* member of the Board; (iii) the Executive Director; (iv) the Privacy Officer; (v) a representative from the Exchange responsible for data and analytics, (vi) an individual with a professional or academic research background; (vii) a representative from the health insurance industry; (viii) an attorney with experience in health care, data privacy or research matters; (ix) a health care professional, such as a physician, nurse, social worker or psychologist; (x) an individual with experience in hospital administration, analytics or research; and (xi) a representative from a State agency (each a “Member” and collectively the “Members”). No more than two (2) Members shall be non-voting members of the Board.
- ii. Appointment and Removal. Members shall be appointed by and serve at the pleasure of the Board. When appointing a Member, the Board shall consider nominations from the Executive Director. The Board may remove and replace Members at any time in the discretion of the Board.
- iii. Voting Rights. Each Member shall have one vote.
- iv. Terms. There shall be no term limits with respect to Members.
- v. Chairperson. The Board shall designate a Member of the Data Release and Review Committee to act as chairperson of the Data Release and Review 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 Committee.

c. Meetings.

- i. The Data Release and Review Committee normally shall meet at least quarterly, or more frequently as circumstances dictate, in accordance with a schedule set by the Executive Director. Meetings not scheduled on a regular basis in advance may be called by the

Executive Director upon reasonable notice provided such notice is not less than five (5) business days. Members may attend a meeting in person or via teleconference; provided that the Member takes reasonable precautions during such teleconference to ensure the confidentiality of the meeting in accordance with this Policy. The Executive Director reserves the right to cancel any scheduled meeting in the event no Data Release Application is available for review and consideration.

- ii. In order to enhance its ability to fulfill its responsibilities, the Data Release and Review Committee may invite to its meetings, or communicate with, any member of the Board, any member of the Advisory Group, any employee of the Exchange or such other persons as it deems appropriate for the purpose of securing additional guidance and information.
- iii. All meetings of the Data Release and Review Committee shall be open to the public, though all deliberations of the Data Release and Review Committee shall be strictly confidential.
- iv. In support of the Data Release and Review Committee's meeting schedule, the Executive Director shall arrange for the preparation of meeting agendas, support materials relevant to the Members' review of Data Release Applications and preparing meeting minutes and circulating such minutes to the Members.

d. Voting.

- i. Voting/Quorum. Three (3) voting Members shall constitute a quorum for the transaction of business, and the vote of a majority of such quorum shall be required for the Data Release and Review 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.

5. Use of Data by the Exchange.

a. Access to Data by APCD Personnel.

- i. The Executive Director shall designate, in writing, Exchange employees, agents and contractors permitted to access Data through the Managed Environment (“APCD Personnel”) based upon such individual’s job description, role at the Exchange and relationship to the APCD. No other individual, regardless of relationship to the Exchange, shall be permitted to access Data through the Managed Environment.
- ii. All APCD Personnel shall be credentialed in accordance with applicable Exchange policies and procedures prior to being granted access to the Data through the Managed Environment. Access to the Data through the Managed Environment shall be subject to the applicable access authentication and audit report requirements of the Exchange’s security program and policies, including but not limited to the use of dual-factor authentication.
- iii. The Executive Director shall review the list of APCD Personnel permitted access to Data through the Managed Environment at least every three (3) months and shall revise as necessary.
- iv. APCD Personnel shall be required to change their password for accessing the Managed Environment every ninety (90) days. APCD Personnel shall be strictly prohibited from disclosing their access credentials, including password, for the Managed Environment to any other individual or entity.

b. Use of the Managed Environment and Data

- i. APCD Personnel may access Data through the Managed Environment only (i) to review and analyze such Data for purposes of fulfilling the Exchange’s mandate under the Act, including but not limited to the preparation of consumer and public-facing reports and analyses, or (ii) for Exchange internal business administration or operations.
- ii. APCD Personnel may not access Data through the Managed Environment, 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.
- iii. When accessing and using the Managed Environment, APCD Personnel shall: (i) never install any software, application or code in the Managed Environment, unless specific written approval has been provided by the Executive Director; (ii) never link external data with

De-identified Data from Managed Environment without prior written approval from the Executive Director; and (iii) not re-identify, or attempt to re-identify, De-identified Data.

- iv. Except as otherwise set forth herein, all Data accessed through the Managed Environment by APCD Personnel shall be De-Identified. Notwithstanding, the Executive Director may, in his or her discretion, permit designated APCD Personnel to access a Limited Data Set from the Managed Environment. APCD Personnel granted access to a Limited Data Set by the Executive Director 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 the Exchange, without the prior written consent of the Executive Director.
- v. The Exchange shall maintain: (i) copies of the Managed Environment output and make such information available for the purpose of conducting security audits; and (ii) Managed Environment access logs.

c. Disclosure of Data by APCD Personnel.

- i. APCD Personnel may not disclose any Data accessed through the Managed Environment 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 and Review Committee; (ii) with the written consent of the Executive Director and after the execution of a written confidentiality agreement between the Exchange and the approved recipient, when such disclosure is reasonably necessary for the Exchange's operations or fulfillment of the purpose of the Act; or (iii) as required by state or federal law, regulation or process and after the execution of a written confidentiality agreement between the Exchange and the recipient.
- ii. Any third-party vendor engaged by the Exchange to maintain, use or disclose the Data shall comply with all applicable Exchange 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 health care data, including but not limited to applicable guidance from the National Institutes of Standards and Technology ("NIST"), including but not limited to NIST Special Publication 800-53 Rev 4; (iii) the third-party vendor's privacy and security policies, procedures and protocols;

and (iv) the Exchange's privacy and security policies, procedures and protocols.

d. Safeguarding Data in the Exchange's Possession.

- i. All Data in the possession or custody of APCD Personnel shall be maintained on the Exchange's network and servers. APCD Personnel shall not maintain or store Data on any personal electronic device or on any personal or unapproved remote or cloud storage platform or application.
- ii. All Data shall be maintained in accordance with applicable Exchange security policies, protocols and procedures.

e. Disposal of Data in the Exchange's Possession.

- i. All Data maintained on electronic media shall be sanitized in accordance with NIST Special Publication 800-88 ("Guidelines for Media Sanitation"), as may be amended or superseded from time to time, and in accordance with Exchange policy and procedure. Such sanitation shall be performed and/or certified by the Exchange's information technology department.
- ii. All Data maintained in paper format shall be shredded, pulverized or otherwise destroyed in a manner that prevents re-identification or re-assembly of the Data.

6. Data Release Application Process.

- a. Data Release Application. The Exchange shall develop and maintain a Data Release Application. The Executive Director 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 the Exchange and be willing to be interviewed by the Data Release and Review Committee.
- c. Data Release Application Processing Fees. The Executive Director shall collect a processing fee for each Data Release Application received and such Data Release Application Processing Fee shall approximate the costs associated with the process of reviewing the Data Release Application. The Executive Director shall create and publish a fee schedule for such processing fees.

- d. Confidentiality. The Executive Director and the Data Release and Review Committee shall take reasonable steps and implement reasonable measures to safeguard the confidentiality of the Applicant and the Data Release Application and shall make public only the information identified in Section 7(f) of this Policy.
- e. Data Release Application Review Process.
  - i. Role of Executive Director.
    - 1. Tasks. Within fifteen (15) calendar days of receipt of a Data Release Application, the Executive Director shall perform the following tasks with respect to his or her review of the Data Release Application:
      - a. Receive Data Release Applications from Applicants.
      - b. Maintain a record of each Data Release Application received.
      - c. Determine if the Data Release Application is complete and the Applicant has provided all information required by the Data Release Application.
    - 2. Right to reject Data Release Application. The Executive Director may reject a Data Release Application in the event the Executive Director, in his or her sole discretion, determines that the Data Release Application is incomplete.
    - 3. Right to request additional information. The Executive Director may request additional information or clarification from the Applicant, including but not limited to requesting a meeting with the Applicant.
    - 4. Submission to Data Release and Review Committee. Within ten (10) business days of the Executive Director's determination that the Data Release Application is complete, the Executive Director shall submit such Data Release Application to the Data Release and Review Committee. Any complete Data Release Applications received from the Executive Director fifteen (15) or more days prior to the Data Release and Review Committee's next scheduled meeting, shall be reviewed and considered at such next scheduled meeting. Any complete Data Release Applications received from the Executive Director less than

fifteen (15) business days prior to the Data Release and Review Committee's next scheduled meeting shall be reviewed and considered at the meeting following the next scheduled meeting. 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 reasonably be able to re-identify 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 Executive Director or Data Release and Review 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.
5. Right to request additional information. The Data Release and Review Committee shall have the right to direct the Executive Director to request additional information, seek clarification from the Applicant or request a meeting with the Applicant. Any such requests shall be communicated to the Executive Director at least five (5) business days prior to the meeting at which the Data Release Application will be considered.
6. Support by Executive Director and Exchange. The Data Release and Review Committee may seek assistance, guidance and technical advice from the Executive Director or the staff of the Exchange at any time during its review and consideration of a Data Release Application. The Data Release and Review 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.

7. Decisions. Upon completion of its review and consideration of a Data Release Application, the Data Release and Review Committee may issue one of the following three decisions:

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

ii. No Right of Appeal. An Applicant may have a right to appeal a decision of the Executive Director or the Data Release and Review Committee.

iii. 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; provided that in the event an Applicant or an Applicant Related Party has, in the sole discretion of the Executive Director or Data Release and Review Committee, previously violated any term or condition of a Data Use Agreement entered into

between the Exchange and such Applicant or Applicant Related Party, the Executive Director may deny such Applicant or Applicant Related Party the opportunity to re-submit an existing, or submit a new, Data Release Application. The Executive Director also has the discretion to deny consideration of a new Data Release Application if upon preliminary review by the Executive Director, the Data Release Application has not materially changed.

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

a. Data Use Agreement.

- i. The Executive Director, in consultation with the Exchange and Data Release and Review 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 the Exchange 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 the Exchange 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 Executive Director 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 Executive Director 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 the Exchange 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 the Exchange 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(e)(7) of this Policy, the Executive Director 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 Executive Director determines that the Recipient has violated any term or condition of the Data Use Agreement, the Exchange 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 Exchange; and/or (v) institute legal proceedings against the Recipient.
- b. Form/Manner of Access. The Exchange shall make Data available to a Recipient through one of two models. The Recipient, in consultation with the Exchange, shall select the model most appropriate for the Recipient and its approved Project and shall ensure in either case that the access is secure.
- i. Transmission. The Exchange shall offer a "Transmission Model" of Data access, pursuant to which the Exchange shall collect, format and transmit the Data approved for release by the Data Release and Review Committee to the Recipient.
  - ii. Enclave Model. The Exchange may offer an "Enclave Model" of Data access, pursuant to which the APCD shall permit Recipients remote access to the Data approved for release by the Data Release and Review Committee. Pursuant to this model, all Data will reside exclusively on Exchange servers.
- c. De-Identification. All Data released to a Recipient shall be De-Identified prior to release and no key, protocol or other information that may reasonably be used to re-identify the Data shall be provided to the Recipient.
- d. Minimum Necessary. The Exchange shall release only the Data the Executive Director and/or Data Release and Review Committee, in

consultation with the Applicant, determines to be the minimum necessary for the Applicant to conduct the Project.

- e. Access Fees. The Exchange, in its discretion, may charge fees to Recipients for access to Data through the Transmission or Enclave Models. In the event such fees are charged, the Executive Director shall create and publish a schedule of such access fees and such fees shall approximate the Exchange's associated costs related to such access.
- f. Posting of Approved Data Release Applications on APCD website. All Data Release Applications approved by the Data Release and Review Committee shall be identified on a website maintained by the Exchange. The Exchange shall include at least the following information on the website for each approved Data Release Application: (i) Applicant name and contact information; and (ii) description and purpose of Project.

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 the Exchange and the Recipient, or at the end of any Project, the Executive Director may require the Recipient, or any Recipient Related Party, to return to the Exchange or destroy any or all Data in the Recipient's or the Recipient Related Party's possession or control. The Executive Director 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 National Institute of Standards and Technology (NIST) Special Publication 800-88 ("Guidelines for Media Sanitation"), as may be amended or superseded from time to time. All Data maintained in paper format shall be shredded, pulverized or otherwise destroyed in a manner that prevents re-identification or re-assembly of the Data.
- c. Certification of Return or Destruction. The Executive Director 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 the Exchange or destroyed in accordance with this Policy.

9. Ownership of Data and Work Product.

- a. Ownership of Data. All Data shall be, at all times and regardless of possession or control by any Recipient or Recipient Related Party, the sole property of the Exchange and no grant of access to such Data through an approved Data Release Application shall be construed to provide the

Recipient or any Recipient Related Party any ownership or property interest in such Data.

- b. Ownership of Work Product. The Exchange 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 (collectively, "Publish"; such a Publishing is a "Publication"), 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").
  - i. Not less than thirty (30) days prior to the earlier of Publication or submission for Publication of any Manuscript, Recipient shall provide the Exchange with a copy of the Manuscript. Recipient shall delete any Data or other information or content that the Exchange requests in writing be deleted because of concerns with the privacy or confidentiality of the subjects of the Data.
  - ii. Any Manuscript must comply with HIPAA's cell suppression policy and include only De-Identified Data.
  - iii. Recipient shall publicly acknowledge in any Manuscript the Exchange's contribution of the Data, and Recipient may use the Exchange's name for that purpose.
  - iv. Recipient hereby grants a worldwide, perpetual, royalty-free, and transferrable license in the Manuscript to the Exchange for the limited purpose of allowing the Exchange to post the Manuscript on its public-facing website or otherwise make the Manuscript publically available. In the event Recipient does not have the legal right to grant such license to the Exchange, the Recipient shall reasonably assist the Exchange in obtaining such license, or an equivalent license, from the appropriate individual or entity.

#### 10. Annual Reporting.

- a. The Data Release and Review Committee shall perform a review and evaluation, at least annually, of the performance of the Data Release and Review Committee, including reviewing the compliance of the Data Release and Review Committee with this Policy. In addition, the Data Release and Review Committee shall review and reassess, at least annually, the adequacy of this Policy and recommend to the Board any improvements

to this Policy that the Data Release and Review Committee considers necessary or valuable.

- b. The Data Release and Review Committee shall submit a report to the Board, at least annually, outlining the Data Release and Review Committee's activities, statistics relating to the volume and type of Data Release Applications received, and the review and acceptance or rejection of Data Release Applications.

11. Conflicts.

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

DRAFT