Connecticut Office of Health Strategy

All-Payer Claims Database

Policy and Procedures Manual

[Date]

Contents

1. Purpose of Policy 3
    a. APCD Legislative Mandate and History 3
    b. Purpose of the Policy 3
2. Definitions 3
3. Office of Health Strategy 6
4. Use of Data by OHS 6
    a. Access to Data by APCD Personnel 6
    b. Use of the Managed Environment and Data 7
    c. Disclosure of Data by APCD Personnel 7
    d. Safeguarding Data in OHS' Possession. 8
5. Use of the Managed Environment and Data 8
6. Disclosure of Data by APCD Personnel. 9
7. Safeguarding Data in the OHS' Possession 10
8. Disposal of Data in OHS' Possession 10
9. Data Release Committee 10
    a. Purpose and Mission 10
    b. Governance 10
    i. Committee Members 10
    ii. Appointment and Removal 11
    iii. Voting Rights 11
    iv. Terms 11
    v. Chairperson 11
    c. Meetings 11
    d. Voting 11
    i. Voting/Quorum 11
    ii. Recusals/Conflicts of Interest 11
    e. Delegation 12
    f. Coordination 12
10. Data Release Application Process 12
    a. Data Release Application 12
    b. Submission 12
    c. Data Release Application Processing Fees 12
    d. Data Release Application Review Process 12

i. Role of HITO 12
ii. Review by Data Release Committee 12
iii. Veto Authority 14
iv. Opportunity for Resubmission of Data Release Application 14
v. Right of Appeal 14
vi. Process to appeal final denial of data request. 15
11. Release of Data Pursuant to Approved Data Release Applications 15
a. Data Use Agreement 15
b. Form/Manner of Access 17
c. De-Identification 17
d. Minimum Necessary 17
e. Access Fees 17
f. Posting of Data Release Application Disposition on APCD Website 17
12. Return or Destruction of Data. 17
a. Return or Destruction of Data 17
b. Standard of Destruction 18
c. Certification of Return or Destruction 18
13. Ownership of Data and Work Product 18
a. Ownership of Data. 18
b. Ownership of Work Product 18
c. Publications 18
14. Annual Reporting 18
15. Conflicts. 19
16. Confidentiality. 19

1. ## Purpose of Policy.

   a. APCD Legislative Mandate and History. Public Act 13-247 enabled the 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 Office of Health Strategy ("OHS") for inclusion in the APCD. The Act allows OHS: (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.

   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 Chapters 368z, 368dd and 368ee of the Connecticut General Statutes, as may be amended from time to time.

   b. "*Advisory Group*" shall mean the All-Payer Claims Database Advisory Group established pursuant to Conn. Gen. Stat. § 17b-59f(e).

   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 Executive Director 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 OHS.

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

g. “*Data*” means claim information provided to the APCD by Data Submitters and made available through the Vendor or Managed Environment.

h. “Data Privacy and Security Subcommittee*”(DPS* means the 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 OHS or the Data Release Committee in connection with a request to access Data.

j. “*Data Release Committee*”(DRC) means the APCD 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. “*Executive Director”* means the Executive Director of the OHS.

o. *“External Procedures*” mean the set of procedures maintained by OHS that detail the processes related to the ability of the DRC to review and act on Data Release Applications.

p. “*HIPAA*” means the Health Insurance Portability and Accountability Act of

1996 and its implementing regulations, each as amended from time to time.

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

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

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

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

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

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

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

x. "*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.

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

z. "*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.

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

3. Office of Health Strategy

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

b. The OHS 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 OHS 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 Executive Director 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 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. 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 trained 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.

iii. The Executive Director shall review the list of APCD Personnel permitted access to Data through the Vendor or Managed Environment at least every six (6) 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 or Vendor only (1) to review and analyze such Data for purposes of fulfilling the OHS' statutory mandate pursuant to Conn. Gen. Stat. Chapters 368z and 368dd, including but not limited to the preparation of consumer and public facing reports and analyses, or (2) for OHS internal administration or operations.

ii. APCD Personnel may not access Data through the Managed Environment or Vendor, or otherwise use or disclose such Data, for (1) any private or illegal purpose, or (2) any purpose inconsistent with the applicable state or federal law or this Policy.

iii. When accessing and using the Managed Environment or obtaining Data through the Vendor, APCD Personnel shall: (1) never install any software, application or code in the Managed Environment, unless specific written approval has been provided by the Executive Director; (2) never link external data with Data from Managed Environment or the Vendor without prior written approval from the Executive Director; and (3) not re-identify, or attempt to reidentify, Data.

iv. OHS shall maintain: (1) copies of the Managed Environment and Vendor output and make such information available for the purpose of conducting security audits; and (2) 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: (1) as explicitly permitted by this Policy, including but not limited to disclosure after approval of a Data Release Application by the Data Release Committee; (2) with the written consent of the Executive Director and after the execution of a Data Use Agreement between OHS and the approved recipient, when such disclosure is reasonably necessary for OHS' operations or fulfillment of the purpose of the Act; or (3) as required by state or federal law, regulation or process.

ii. Any third-party vendor engaged by the 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: (1) the specifications and requirements set forth in applicable State and federal law; (2) industry standards and best practices regarding the maintenance and security of healthcare 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, as may be amended or superseded from time to time; (3) the third party vendor's privacy and security policies, procedures and protocols; and (4) OHS' privacy and security policies, procedures and protocols.

d. Safeguarding Data in OHS' Possession.

i. All Data in the possession or custody of APCD Personnel shall be maintained on the OHS'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 OHS security policies, protocols and procedures.

5. Use of the Managed Environment and Data

a. APCD Personnel may access Data through the Managed Environment or Vendor only (1) 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 (2) for OHS internal business administration or operations (3) including preparing deidentified extracts for delivery to external researchers and preparing Limited Data Sets for internal, state-driven research. Any access of Data by APCD Personnel inconsistent with this Policy will be subject to OHS personnel policies.

b. All Data accessed through the Managed Environment or Vendor 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 or Vendor. 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 OHS without the prior written consent of the Executive Director.

c. APCD Personnel may not access Data through the Managed Environment or Vendor, or otherwise use or disclose such Data, for (1) any private or illegal purpose, or (2) any purpose inconsistent with the Act or this Policy.

d. When accessing and using the Managed Environment or obtaining Data through the Vendor, APCD Personnel shall: (1) never install any software, application or code in the Managed Environment, unless specific written approval has been provided by the Executive Director; (2) never link external data with Data from Managed Environment or the Vendor without prior written approval from the HITO; and (3) not re-identify, or attempt to reidentify, Data.

e. OHS shall maintain: (1) copies of the Managed Environment and Vendor output and make such information available for the purpose of conducting security audits; and (2) Managed Environment and Vendor access logs.

6. Disclosure of Data by APCD Personnel.

a. 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 Executive Director and after the execution of a written data use 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.

b. 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.

7. Safeguarding Data in the OHS' Possession.

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

8. Disposal of Data in OHS' Possession.

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

b. 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.

c. OHS must receive a data destruction attestation after two weeks of project completion for any entity working on internal, state-driven research.

9. Data Release Committee.

a. Purpose and Mission. The purpose of the Data Release Committee shall be to: (i) review and approve or deny Data Release Applications submitted by Applicants for the release of Data; and (ii) provide support to the OHS 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: (a) The Medicaid Director or his/her designee; (b) The Department of Mental Health and Addiction Services (DMHAS) Commissioner or his/her designee; (c) the Executive Director or designee; (d) an individual with a professional or academic research background involving public health matters; (e) a representative from the health insurance industry; (f) an attorney with experience in health care, data privacy or research matters; (g) a healthcare professional, such as a physician, nurse, social worker or psychologist; (h) an individual with experience in hospital administration, analytics or research; and (i) 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 Committee Chair.

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.

10. Data Release Application Process.

a. Data Release Application. OHS 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; 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. OHS shall collect a processing fee for each Data Release Application received. OHS 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, or designee, 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, or designee, 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. *Application Review*: Upon receipt of a Data Release Application from OHS, 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 OHS 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 OHS 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 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. 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. OHS also has the discretion to deny consideration of a new Data Release Application if upon preliminary review by OHS, the Data Release Application has not materially changed.

v. Right of Appeal.

a. An Applicant may request an administrative review of a data request denial decision by the Executive

Director or the Data Release Committee. A written request for an administrative review may, within 30 calendar days after notice of the denial, be filed with Data Release Committee. The request should include, at minimum:

i. data requestor's name, address, telephone number, email address and contact person;

ii. Information about the subject of the review including remedy requested;

iii. A detailed explanation of the issue in dispute and a rationale for a reconsideration of the denial decision.

b. The Executive Director or director's designee will review the administrative review petition. The reviewing official may request additional information or a conference with the Applicant. A decision from the reviewing official will be provided in writing to the Applicant no later than 30 calendar days after receipt of the request. A denial of the request will include the reasons for the denial.

vi. Process to appeal final denial of data request.
An Applicant may have a right to appeal a decision on a Data Release Application made by the Executive Director or the Data Release Committee, in accordance with the provisions of Chapter 54 of the Connecticut General Statutes. Such request for appeal must be submitted in writing to the Data Release Committee within 15 calendar days after receipt of written notification of denial of the administrative review, with a copy provided to the Executive Director.

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

a. Data Use Agreement.

i. OHS, in consultation with 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 OHS 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 OHS 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 10(d)(ii)(4) of this Policy, OHS 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 that OHS 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 applicable, 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 OHS 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, OHS 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. OHS, 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 including any key, protocol or map that would allow the Data to be re-identified.

d. Minimum Necessary. OHS shall release only the Data it and/or the 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, OHS shall create and publish a schedule of such access fees.

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

12. 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, OHS 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. OHS reserves the right, in its 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. OHS may require, in its 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.

13. 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, except as otherwise stated in the Data Use Agreement.

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 detailed in each Project's Data Use Agreement.

14. 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.

15. 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.

16. 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.