Healthcare Payments Data Program Review Committee

September 19, 2019

Office of Statewide Health Planning and Development

2020 W. El Camino Avenue, Sacramento, CA, 95833

Conference Room 1237

OSHPD
Office of Statewide Health Planning and Development

Welcome and Meeting Minutes

Ken Stuart, Chair, Review Committee

Deputy Director's Report

Scott Christman,

Deputy Director and Chief Information Officer,

OSHPD

Follow Up from August 15 Meeting

HPD Data Quality and Improvement – Part 2

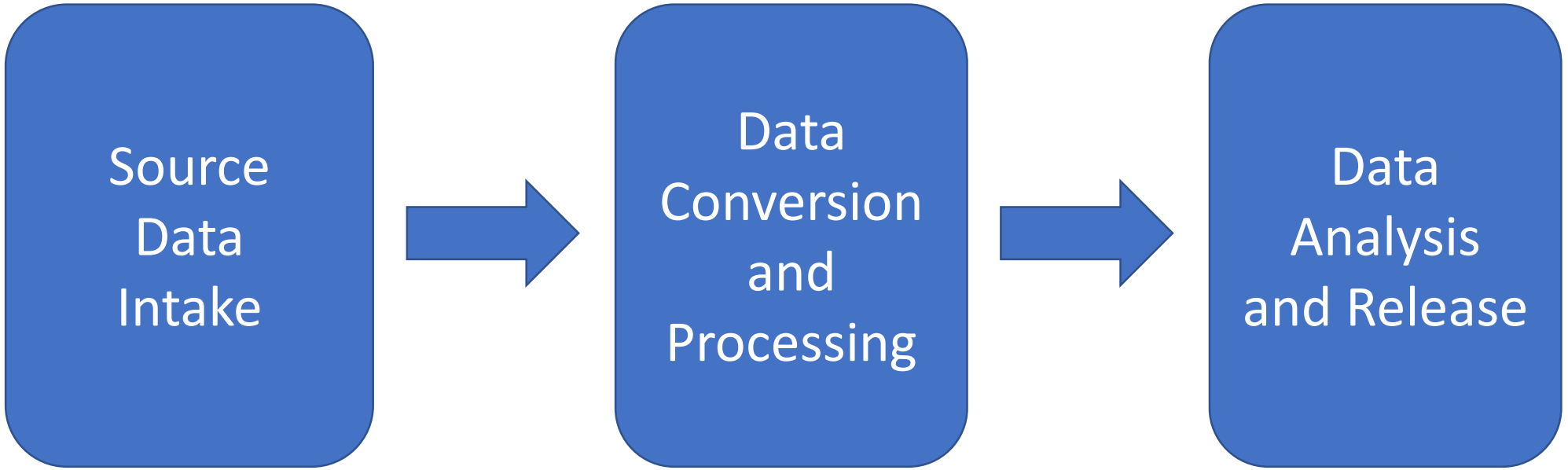
HPD Review Committee Meeting

Jonathan Mathieu

September 19, 2019

OSHPD
Office of Statewide Health Planning and Development

Data Quality throughout the Life Cycle



Recommendation:

1. Establish HPD Data Quality and Improvement Processes

1. The Review Committee recommends that the HPD Program develop transparent data quality and improvement processes. In developing the program, OSHPD shall review and leverage known and effective data quality improvement processes and experiences.

August action: Approved 10 – 0

Recommendation:

2. Multi-Phase Data Quality and Improvement Processes

2. The Review Committee recommends that data quality processes should be applied to each major phase of the HPD data life-cycle, including:
   a) Source data intake
   b) Data conversion and processing
   c) Data analysis, reporting, and release.

August action: Approved 10 – 0

Recommendation:

3. Resubmission Requirements

3. The Review Committee recommends that the HPD Program have authority to require resubmissions if data fail to meet established data quality standards.

August action: Withdrawn – Review Committee agreed this was sufficiently reflected in a revised Recommendation #1.

Recommendation:

4. Stakeholder Data Quality Information

4. The Review Committee recommends that the HPD Program provide stakeholders with accessible information on data quality, including:
   a) Descriptions of processes and methodologies
   b) Periodic updates on known issues and their implications.

August action: Postponed discussion and vote due to time constraints

OSHPD Current Data Privacy and Governance Practices

Scott Christman, Deputy Director and Chief Information Officer,

OSHPD

Today's Topics

- Information Security at OSHPD
- Current Data Collection
- Access to Non-Public Data Sets
- Governance and Security of Non-Public Data Sets

OSHPD Information Security Program

- OSHPD follows Federal standards such as the NIST Cybersecurity Framework and California ISO security policies and standards.
- Key information security practices:
  - Multiple layers of security to avoid single points of failure
  - Use of validated software for encryption at rest and in-transit
  - Role based access configured for least privilege and separation of duties
  - Continuous monitoring for security compliance
  - Regular external assessment of OSHPD information security practices
    - In March 2019, the California Military Department performed an information security assessment. This included a broad vulnerability assessment and an attempted penetration into OSHPD systems and network.

Current Data Collection – Personal Information

- Existing law requires health facilities to file reports with OSHPD.
- Patient level reports include the:
  - Inpatient Discharge Data
  - Emergency Department Encounter Data
  - Ambulatory Surgery Encounter Data
  - Coronary Artery Bypass Graft Data
- OSHPD is required to provide this information to specified entities under law, in addition to aggregate public reporting

Access of Non-Public Data Sets

- Research Data – Information Practices Act
  - Subject to “minimum variables necessary” standard to meet the intent of the research project
  - University of California and nonprofit educational institutions are eligible to receive data under this provision, or in the case of education-related data, any other nonprofit entity conducting scientific research
  - Projects must be approved by the Committee for the Protection of Human Subjects (CPHS) Institutional Review Board (IRB)
- HIPAA Limited Data – Health Data Act
  - OSHPD offers several types of non-public record-level data to licensed California Hospitals and California Local Health Departments.
  - Eligible hospitals and local health departments may request Limited Data Sets for PDD, EDD, and ASD datasets
- Aggregated Reporting – Health Data Act / OSHPD Mission
  - Custom reports or analyses provided to public requestors, such as media
  - Interactive Web-Based Reports developed by OSHPD on specified topics of import and published on the open data portal
  - Data is aggregated by facility, county, or otherwise de-identified per CHHS Agency data de-identification standards

Governance and Security of Non-Public Data Sets

- All data releases require a data use agreement with the recipient
- Data recipients are required to certify their IT environments meet specified security requirements; requirements reviewed and updated annually by OSHPD
- Data transmitted to recipients using secure file transfer protocols
- Data recipients are required to notify OSHPD of any data breaches or misuses
- Data recipients are required to return/destroy data upon completion of analysis and notify OSHPD
- OSHPD monitors public inappropriate uses of the data, works with data requestors to educate and inform them about appropriate data uses

Data Privacy and Security

Karen Boruff, Consultant,
OSHPD
Jonathan Mathieu, Senior Health Care Data/Policy Consultant,
Freedman HealthCare

Today's Topics

- What is the legal environment that both data submitters and the HPD operate within?
- What are the privacy considerations for data collection, use, and dissemination?
- How do existing California security laws and standards protect personal information?

Our "ask:"

- Provide guidance from a "big picture" perspective
- Address details in regulation, policy development and implementation

Privacy-Related Information Requirements

To achieve desired use cases, the HPD will need to:

- *Collect*, *use*, and *release* information about the use of health care services
- Use new technical solutions to complete analyses and publish/post reports and other analytic products based on collected data
- Link HPD data with other datasets to support certain use cases
- Maintain a cross-reference based on direct identifiers for individuals across source datasets (e.g., master person index)
- Provide access, *with appropriate processes and safeguards*, to data for external users such as researchers

Legal Environment of APCDs and Privacy Laws

Federal Privacy-Related Laws

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)*
  - HPD submitters are subject to HIPAA – mandatory submitters meet "required by law" exception, but voluntary submitters cannot legally be compelled to submit data
  - OSHPD is not a covered entity, thus not subject to HIPAA but…
    - HIPAA Privacy & Security Rules may serve as guidelines for defining what data needs to be protected and how.
    - CA state laws and policies overlap with many of the protections and, in many cases, are more protective than HIPAA

*Includes provisions added by the Health Information Technology for Economic and Clinical Health Act (HITECH)

Federal Privacy-Related Laws

- 42 CFR Part 2 – Confidentiality of Substance Use Disorder Patient Records
  - Prohibits disclosure (or redisclosure) of patient-identifying SUD treatment information held by a Part 2 program without patient authorization
  - Legal exceptions are extremely limited – many state APCDs do not collect Part 2 data
  - Ongoing efforts at federal level to clarify requirements and align with HIPAA to support research and care coordination

California Privacy-Related Laws

- Confidentiality of Medical Information Act (CMIA)
  - Authorization from patient is required for disclosures except for treatment, payment, operations or when required by law
  - OSHPD is not subject to CMIA, but majority of submitters are – as with HIPAA, mandatory submitters meet “required by law” exception, but voluntary submitters cannot legally be compelled to submit data
- Lanterman-Petris-Short Act (LPS)
  - Prohibits disclosure of certain mental health information without authorization except in limited circumstances e.g., payment or healthcare operations
  - Mandate to submit data to HPD will meet legal exception, giving submitters appropriate authority

California Privacy-Related Laws

- Information Practices Act (IPA)
  - OSHPD is subject to IPA
  - Prohibited from disclosing personal information except in certain circumstances
  - In the absence of specific language in statute, OSHPD would be limited to releasing data only as described by IPA
- California Public Records Act (PRA)
  - AB 1810 specifically exempts the HPD: "…individual patient-level data shall be exempt from the disclosure requirements of the California Public Records Act."

The IPA requires state entities to "establish appropriate and reasonable ***administrative, technical, and physical safeguard***s to ensure…the security and confidentiality of records, and to protect against anticipated threats or hazards."

State administrative manuals outline the standards that all state agencies must follow in order to comply with the IPA.

Data Submission and Collection

Data Submission: Authority for Submitters

Mandatory Submitters	Authority
• Commercial Health Plans • Medicare Advantage • Self-insured non-ERISA • Dental insurers	• HIPAA and CMIA “required by law”
• Medi-Cal managed care & Fee For Service (via DHCS)	• Social Security Act • HIPAA – required by law, research, or public health • Welfare & Institution Code • Information Practices Act

Data Submission: Authority for Submitters

Voluntary Submitters	Authority
• ERISA self-insured plans • Private Taft-Hartley Trusts • Federal Health Benefits	• HIPAA health oversight or public health activities • CMIA public health or bona fide research
• Medicare Fee For Service	• HIPAA research (broad interpretation) through State Agency Research Request • Affordable Care Act to measure provider performance through Qualified Entity Certification Program

Other State APCD Experience – Data Submission

- Covered Entities are familiar/comfortable operating under HIPAA
- Have policies, procedures, and staff to ensure compliance
- More willing to submit data under Required by Law/Public Health exceptions
- APCD purposes established in enabling statute and regulations

Data Collection: Authority for OSHPD

- Authority provided to OSHPD through Data Act does not cover authority to collect personal information from submitters and operate the HPD
  - Legislation is needed to clearly identify OSHPD's role and authority
- Other state APCDs typically name the state organization responsible for administering the APCD in the enabling legislation
  - Specifies purposes, e.g., public health, research, policy, health care operations, and "Triple Aim"-type goals: better care, better health, lower cost

Data Collection: CMS (Medicare FFS)

- OSHPD may request data from CMS via one of the following:
  - State Agency Request Process – single state agency may request data for research purposes, including a broad range of analytic activities (e.g., multi-payer analysis possible with an APCD)
  - Qualified Entity Certification Program – entity may request and use the data to generate performance reports for providers using approved measures of quality, efficiency, effectiveness, and resource use. Re-release of record level data to “authorized users” is also permitted
- Majority of state APCDs use the State Agency Request Process

Data Collection: DHCS (Medi-Cal)

- OSHPD is authorized to collect data from DHCS per the following:
  - HPD assists Medi-Cal with meeting their requirements for evaluating and administering the program – meets SSA requirements for data sharing
  - HPD supports public health purposes – meets HIPAA requirements for DHCS as a covered entity
  - Pursuant to IPA, OSHPD will require the data to conduct its statutory duties
  - Pursuant to the CHHS Data Sharing Framework with an approved Business Use Case Proposal

BREAK

Access and Release

Purpose of Use: Legislative Intent

The HPD should make the purposes for use clear in legislation, and evaluate future requests against that purpose.

HSC, Div. 107, Part 2, Chapter 8.5. Health Care Cost Transparency Database [§127671]

(a) It is the intent of the Legislature in enacting this chapter to establish a system to collect information regarding the cost of health care. Health care data is reported and collected through many disparate systems. Creating a process to aggregate this data will provide greater transparency regarding health care costs, and the information may be used to inform policy decisions regarding the provision of quality health care, reduce disparities, and reduce health care costs.

(b) It is the intent of the Legislature to improve data transparency to achieve a sustainable health care system with more equitable access to affordable and quality health care for all.

(c) It is the intent of the Legislature in enacting this chapter to encourage health care service plans, health insurers, and providers to use such data to develop innovative approaches, services, and programs that may have the potential to deliver health care that is both cost effective and responsive to the needs of enrollees, including recognizing the diversity of California and the impact of social determinants of health.

(Added by Stats. 2018, Ch. 34, Sec. 23. (AB 1810) Effective June 27, 2018.)

Other State APCD Experience – Data Release

- Enabling legislation establishes what data can be released, to whom, and for what purposes
- APCDs are not subject to but generally follow HIPAA
  - Types of data released – e.g., de-identified data, limited data sets, identified data
  - Legal framework – data use agreement (DUA), minimum necessary, alignment with policy goals

Other State APCD Experience – Data Release

- Custom/Standard Reports, Public Use File, De-Identified Data Set
  - Produced by APCD Administrator
  - No PHI – no/very low patient privacy risk
  - Simple application, expedited review and approval process
  - DUA sometimes used to protect APCD interests and limit uses, sale, or re-distribution

Type	Description
De-Identified Data Set, Public Use File	Aggregated or record level data sets that satisfy the HIPAA standard for de-identification. Can be standardized or custom.
Custom Reports or Analyses	Summary of results based on analysis of a particular issue/set of questions. Often requested by researchers, lawmakers, and policymakers
Standard Reports	Reports on specific topics, regularly updated. Topics include health care cost/utilization, hospital readmissions, ED use, Rx spending, etc.

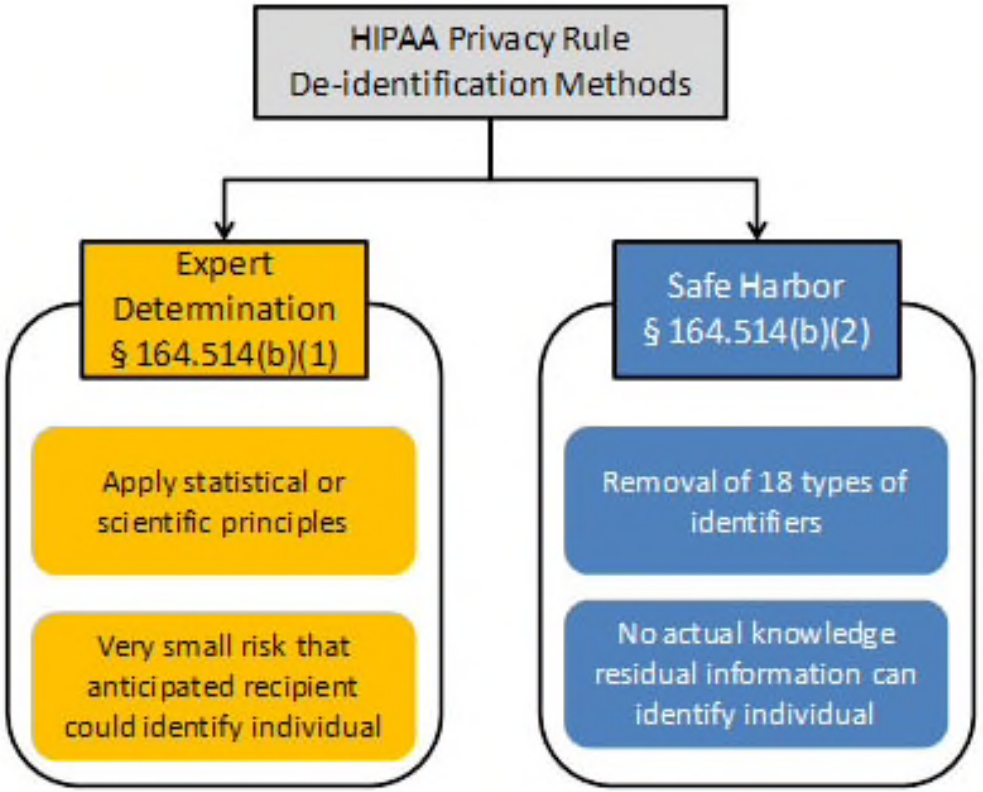
Other State APCD Experience – Data Release

- Limited Data Set/Identified Data
  - Include PHI – moderate/high patient privacy risk
  - More detailed application, enhanced review and approval process
  - Independent Data Release Committee reviews applications, makes approval recommendations
  - IRB or Privacy Board review/approval may be required
  - Requestor required to justify/demonstrate need for PHI
  - HIPAA-compliant DUA required

Type	Description
Limited Data Set	Provided for specific purposes. Aligned with HIPAA exceptions for research, public health and operations uses. Contains PHI but no direct identifiers.
Identified Data	Very limited users and uses – research and operations. Contains PHI (indirect and direct identifiers)

De-Identified Data

- HIPAA standard – “health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable information.”
- CHHS De-Identification Guidelines – “aggregate data” is “collective data that relates to a group or category of services or individuals. The aggregate data may be shown in table form as counts, percentages, rates, averages, or other statistical groupings,” and meet the requirements of the IPA and HIPAA to prevent the disclosure of personal information.



Identifiable Data

- Record-level data – information specific to a person
  - Identifiable data may or may not include direct identifiers. Could be used, along with other sources, to identify specific individuals.
  - Due to risk of identifying individuals, assessment of identifiability is required
- HIPAA Limited Data Set – type of identifiable data set
  - Includes some PHI but removes direct identifiers to reduce the risk of reidentification

The HIPAA Limited Data Set Removes the Following Direct Identifiers

1. Names
2. Postal address information, other than town or city, State, and zip code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images

Identifiers in white *are* found in claims and encounter data, others are not.

Information Security

California Requirements

- State information security requirements
  - IPA: requires state entities to “establish appropriate and administrative, technical, and physical safeguards to ensure…the security and confidentiality of records, and to protect against anticipated threats or hazards”
  - Gov Code: state entities are required to comply with information security and privacy policies, standards and procedures issued by the California Information Security Office (CISO).
- California Department of Technology has broad responsibility and authority over all aspects of technology in California state government

CISO Security and Privacy Standards

- State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM)
  - Contain the information security policies and standards required for all state entities in accordance with IPA
  - Standards set by CISO adopt most, if not all, industry standards for information security

National Institute of Standards and Technology (NIST)

- 800-53 – Security & Privacy Controls
- 800-34 – Contingency Planning Guide
- 800-150 – Guide to Cyber Threat Information Sharing

Federal Information Processing Standards (FIPS)

- FIPS 199 – Standards for Security Categorization
- FIPS 200 – Minimum Security Requirements
- FIPS 140-2 – Security Requirements for Cryptographic Modules

Existing California Information Security Requirements – Implications for the HPD

- California laws and practices require the HPD to adhere to high standards for information security and privacy
  - Subject to IPA and CISO standards
  - Overlap with and are more stringent than HIPAA Rules
  - Other standards address collection limitation, privacy, and breach notification requirements

Recommendations

Recommendation:

1. Privacy Principles

1. The Review Committee recommends the HPD Program adopt the following principles:
   a) The HPD shall protect individual privacy in compliance with applicable federal and state laws.
   b) The HPD is established to learn about the health care system, not about individuals.
   c) The purpose of the HPD is to serve the intent of the Legislature.

Recommendation:

2. Authority to Collect

2. The Review Committee recommends that legislation clearly authorize data submitters to send, and OSHPD to receive, personal information to meet the legislative intent of the HPD.

To support the submission of data by voluntary submitters, legislation should clearly specify public health as one of the intended uses of the HPD.

Recommendation:

3. Access to HPD Data

3. The Review Committee recommends that only aggregate de-identified information will be publicly accessible. OSHPD should develop a program governing access to non-public HPD data, including a data request process overseen by a data access committee.

Recommendation:

4. Information Security

4. The Review Committee recommends the HPD program develop an information security program that uses existing state standards and complies with applicable federal and state laws.

Appendix

Privacy-Related Provisions

Legislative Report:

- "Analyzes data aggregation and the protection of individual confidentiality to advise on privacy and security." §127672(d)(1)(D)
- Includes recommendations about:
  - "Legislation needed to protect individual privacy rights and confidentiality of the data." §127672(d)(2)(B)
  - "How the database can map to other datasets, including public health data sets on morbidity and mortality, and data regarding the social determinants of health." §127672(d)(2)(F)

Implementation:

- All policies and procedures developed in the performance of this chapter shall ensure that the privacy, security, and confidentiality of individually identifiable health information is protected." §127673(e)
- "The office shall develop policy regarding data aggregation and the protection of individual confidentiality, privacy, and security. Individual patient-level data shall be exempt from the disclosure requirements of the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code), and shall not be made available except pursuant to this chapter or the Information Practices Act of 1977 (Chapter 1 (commencing with Section 1798) of Title 1.8 of Part 4 of Division 3 of the Civil Code) until the office has developed a policy regarding the release of that data." §127673(f)

APCD Analytics / Products

Type of Release	Type of Data	Audience
Analytic Products: analytic reports or products on specific topics, typically prepared by the state's APCD administrator.	Aggregate De-Identified	Public
Standard Reports: sets of regularly updated aggregate reports of healthcare cost and utilization, such as hospital admission rates, primary care visits, spending on prescription drugs, etc.	Aggregate De-Identified	Public
Interactive Web-Based Reports: aggregate reports of healthcare cost and use, usually made available on a portal, that allow users to perform limited filtering and drill-down capabilities.	Aggregate De-Identified	Public
Custom Reports or Analyses: custom analyses requested by lawmakers, researchers, or the public, usually performed by the state APCD administrator.	Aggregate De-Identified	By request
Record-Level Data Sets: Record level data refers to information that is specific to a person or entity. For example, a record for Jane Doe may include demographics and information on healthcare services, such as a diagnosis or procedure code.	Identifiable	By request; usually researchers

APCD Data Release in 14 States

State APCD	Public Use or De-Identified Data Sets	Limited Data Set	Identified Data	Custom Reports/ Data Sets
Arkansas	x	x		x
Colorado	x	x	x	x
Connecticut	x	x		x
Delaware	x	x	x	x
Maine	x	x	x	
Maryland		x		
Massachusetts		x	x	
Minnesota	x			
New Hampshire	x	x	x	x
Oregon	x	x	x	x
Rhode Island	x	x		
Utah		x	x	
Virginia	x			x
Washington		x		x

California Privacy-Related Laws

- California Consumer Privacy Act (CCPA) of 2018
  - Places protections on consumer's personal information collected and/or held by businesses
  - CCPA defines business as
    - a corporation organized/operated for the profit or financial benefit of its shareholders
    - Buys, receives (for commercial purposes), sells, or shared (for commercial purposes) the personal information of consumers
    - Derives 50% or more of annual revenue from selling consumers' personal information
  - CCPA specifically exempts medical information or PHI, or provider of health care or covered entity governed by CMIA or HIPAA – not applicable to HPD

Public Comment

Upcoming Review Committee Meeting : October 17, 2019