



Leading health system improvement

All-Payer Claim Database

**Data Policy Advisory Committee**

**SUMMARY OF RECOMMENDATIONS**

# APCD Data Policy Advisory Committee

## SUMMARY OF RECOMMENDATIONS

---

### Introduction

In early 2014, Washington state passed Engrossed Second Substitute House Bill 2572, calling for the establishment of an All Payer Claims Database (APCD). The APCD legislation enacted aims to achieve the following primary objectives:

- Assist patients, providers and hospitals to make informed choices about care;
- Enable providers, hospitals and communities to improve by benchmarking their performance against that of others by focusing on ‘best practices;’
- Enable purchasers to identify value and build expectations into their purchasing strategy and reward improvements over time; and
- Promote competition based on quality and cost.

As part of the Centers for Medicare & Medicaid Services (CMS), Center for Consumer Information and Insurance Oversight, Health Insurance Rate Review Grant Program, Cycle III grant, the Office of Financial Management (OFM) contracted with the Washington Health Alliance (Alliance) to convene two ad hoc advisory committees as follows:

#### **Data Policy Advisory Committee (referred to in OFM contract as Strategic Data Work Group)**

The Data Policy Advisory Committee provided technical advice on operational requirements for the All Payer Claims Database that covered such topics as: privacy/security; data submission; business associate agreements; and data use agreements.

#### **Data Release Advisory Committee (referred to in OFM contract as Data Release Work Group)**

The Data Release Advisory Committee provided technical advice on data release requirements for the All Payer Claims Database that covered such topics as: data request application policy; data application review policy; and the data application appeal policy.

Committee members<sup>1</sup> were selected from a cross section of stakeholders from payer, provider, purchaser and consumer organizations. In addition, the committees also included Washington state agency health care data experts as well as academic researchers. Committee members are recognized leaders and/or subject matter experts in areas critical to the operations of a statewide APCD including: health care data privacy and security, data quality, data release and data use. Linda Green of Freedman Healthcare served as facilitator for all working sessions of both committees. Ms. Green is a nationally recognized expert and consultant in all aspects of APCD development and operations.

Both committees were initiated on September 4, 2014 at a joint meeting. The Alliance convened a total of ten working sessions between September 2014 and January 2015. Each session focused on major topic areas of APCD operations and governance as outlined in Appendix 3. It was decided that keeping each Committee informed about its counterpart’s discussions would add value to the process. Every

---

<sup>1</sup> See Appendix 1 for list of committee membership

meeting included a summary and review of both Committees' discussions and recommendations from the previous month. The final meeting held January 16, 2015 was conducted as a joint session to review, discuss and confirm both committees' final recommendations.

Committee meetings were held in the Alliance offices with live, interactive webinar stream for members unable to attend in person.

## **Purpose of the Document**

The purpose of this report is to convey the recommendations of the Data Policy Advisory Committee regarding the implementation and operation of the APCD. This document captures key committee recommendations, discussion and follow-up items if applicable.

Recommendations are categorized into the following two major topic areas: Data Submission and Data Collection, and Data Management (including Data Use Agreements). Included in the appendix are materials specifically created for the committee meetings and other outside source materials that further illustrate the topics and, in several instances, identify "best practices." Also included throughout the document are the Alliance's additional recommendations, based on our experience as an APCD administrator. The Alliance's recommendations are clearly identified.

Recommendations in this document fall into three categories: Rule, Contract, and Policy/Procedure. As the project moves forward, some recommendations may be considered by OFM in the state's rule making process, while others may be better suited for policy and procedure, or the contract between OFM and the lead organization.

The topics addressed by the committee were framed by the contract statement of work and consultative input from Freedman Healthcare; in addition, committee members themselves suggested discussion topics.

# APCD DATA MANAGEMENT RECOMMENDATIONS

## I. Data Submission and Collection

Data submission and collection are foundational components of an APCD.<sup>2</sup> Successful reporting from an APCD begins with receiving timely, accurate data from each data supplier. Committee recommendations largely focused on identifying the data suppliers, defining the criteria for data submission, and identifying how to monitor or manage the compliance of the data suppliers. The committees studied and discussed operational “best practices” in order to make the recommendations that follow below.

### 1. DEFINITION OF DATA FILES THAT SUPPLIERS SUBMIT TO DATABASE

**RECOMMENDATION I.1A: The lead organization should create a formal data submission guide with input by data submitters.**

Recommendation for Rule
<p>Discussion: The OFM rule should direct the lead organization to develop a data submission guide that describes the required schedules, data file format, record specifications, data elements, definitions, code tables and edit specifications, instructions and other technical specifications for payer submission of eligibility data files, medical and pharmacy claims data files, and provider data files to the APCD.<sup>3</sup></p> <p>Committee members discussed evolving efforts to create generic national APCD data specification standards (e.g. Post Adjudicated Claims Data Reporting (PACDR)). These efforts are attempting to support and simplify data submissions required by national carriers to a growing number of state APCDs. While these efforts are evolving, the specifications typically support a bare minimum field list and often do not fully support reporting and analytic needs of states and communities. In addition many data integration vendors supporting APCD implementations have their own data submission standards based on their product capabilities. As such, many vendors are beginning to adopt portions of the national standardization efforts as part of their overall data specifications.</p>

<sup>2</sup> A comparative best practice document is linked in Appendix 2, Item 1.

<sup>3</sup> Two sample data submission guides are attached in Appendix 2, Item 2.

**RECOMMENDATION I.1B: The Data Submission Guide should be developed to allow flexibility for future changes.**

Recommendation  
for Rule

Discussion: The OFM rule should refer to the data submission guide as opposed to including the details in rule. The Committees and the Alliance agree that this will allow for the greatest flexibility when making required, timely changes to the data submission guide. In addition, the Data Submission Guide will not be developed until the necessary infrastructure is in place, including selection of a lead organization and convening formal oversight committees (Data Release and Data Policy). Referring to the guide allows the state to complete rule writing without the dependency on finalizing a data submission guide.

Most states' APCD laws reference the data submission guide rather than include it in rule. Rhode Island and Colorado are examples of states that have rules that refer to data submission guidelines.

**RECOMMENDATION I.1C: The Data Submission Guide should be reviewed routinely and updated as needed, but no more than once per year.**

Recommendation  
for Rule

Discussion: The OFM rule should state a clear intent to update data submission requirements on a periodic basis. The Committee discussed the need for the data submission guide to be modified to respond to changing needs of the data requestors and to respond to industry or marketplace changes. Examples of changes may include: addition of new fields, changes to file layout and field format, and other technical data submission guidance. Because these changes require a level of effort by data suppliers, the Committee agreed that changes (if needed) should not be made more than once annually. The OFM rule should also require the lead organization to conduct a review process with data submitters prior to making any changes.

**RECOMMENDATION I.1D: Require data submitters to conform to the data submission guide as issued by the lead organization and submit data on a timely basis.**

Recommendation  
for Rule

Discussion: The OFM rule should clearly state that the lead organization will establish data submission timelines and data quality standards on behalf of OFM. Submitting data based on a predictable timeline and ensuring data suppliers submit data on time will allow the lead organization to produce timely and relevant reports. As the data submission guide is developed, it will be important to determine the frequency with which data should be submitted (e.g. monthly, quarterly, or semi-annually) based on the desired uses of the APCD, ability of data suppliers to prepare data, ability of the lead organization and data vendor to process the data, and availability of funding supporting the APCD.

**RECOMMENDATION I.1E: Create a Technical Oversight Committee to balance collection of desired data elements with the availability of data and ease of collection.**

Recommendation for Policy and Procedure

Discussion: The lead organization should convene a Technical Oversight Committee that should in turn create policies to ensure fair and equitable treatment of both data suppliers and requestors. It is recommended that data requests be part of a feedback loop to inform future additions to data elements. Committee members highlighted the importance of these mechanisms to be able to respond to changing needs.

The Technical Oversight Committee should be comprised of individuals who are very knowledgeable about claims data, including what data health plans have available. For example, a data requester may wish to have socioeconomic indicators and/or race, ethnicity and language indicators associated with claim data in a data extract from the APCD. However, most commercial health plans, major contributors of data to the APCD, do not capture this type of information as it is not relevant to claims processing. In order to fulfill the desire for this type of information, the Technical Oversight Committee might look to other sources of information, such as census data, that can be added to the APCD, or ensure the extract provides a means to create linkages to data external to the APCD. This, of course, assumes all patient privacy and security requirements are met.

**2. MANDATORY DATA SUBMISSION REQUIREMENTS AND COMPLIANCE**

**RECOMMENDATION I.2A: Establish a Data Submitter Registration process.**

Recommendation for Contract

Discussion: The Data Submitter Registration process would establish the means by which the lead organization knows which entities operating in the state are required to submit data to the APCD. All organizations required to submit data to the APCD would be required to register with the state and/or lead organization. The registration process should include at a minimum:

- a) Primary and secondary contacts;
- b) Data suppliers who are newly offering coverage in the state;
- c) The process for submitting an additional feed;
- d) Changes to data submission by an existing carrier;
- e) Changes to data submitter contact information.

See Appendix 2 - Item 3 for an example registration form.

**RECOMMENDATION I.2B: Allow ample time for data suppliers to comply with Data Submission Guideline changes.**

Recommendation for Rule

Discussion: The OFM rule should direct data suppliers to comply with Data Submission Guide changes and updates within four months of publication. The committees discussed the need to provide ample time for data submitters to respond to changes to the data submission guide. Stakeholders familiar with the technical challenges of responding to changes suggested that four months should be allowed for data submitters to make changes, test and deliver the data with the required changes.

**RECOMMENDATION I.2C: Data submission compliance should be tracked by the lead organization.**

Recommendation for Policy and Procedure

Discussion: The lead organization should create policies and procedures for real-time tracking of data suppliers' compliance with data submission requirements. This interaction between the APCD lead organization and data managers allows real-time troubleshooting of problems. The lead organization should routinely provide compliance reports to data suppliers and OFM.

**RECOMMENDATION I.2D: Drive data submission compliance through collaboration.**

Recommendation for Policy and Procedure

Discussion: The lead organization should create policies to support collaboration with data suppliers. The Committees and the Alliance preferred collaboration with data suppliers through personal outreach when addressing a deficient or delinquent data submission to improve the process for the future.

In instances where data suppliers are delinquent or non-conforming to the Data Submission Guide, the lead organization may allow a grace period (the Committees suggested 22 business days) to allow the data submitter time to attempt to fix the compliance gap. If the mandatory data submitter fails to resolve the requests for compliance, the lead organization should discuss the matter with OFM and determine whether further action is necessary depending on the circumstances.

**RECOMMENDATION I.2E: Establish penalties for non-compliance.**

Recommendation for Rule

Discussion: The OFM rule should create penalties in rule for non-compliant data submitters. Examples of non-compliance include: late data submissions, incomplete data submissions, incorrect format data submissions, and failure to re-submit data when errors are identified by the lead organization or data vendor.

The Committees discussed the fact that non-compliance is a failure for the APCD because data is unavailable for use. In addition, a significant amount of time and energy may be spent adjudicating disputes.

Committee members also believed there could be valid reasons for a data supplier to be non-compliant with the data submission guide. For example, if the data submission specifications required certain data elements be submitted and an organization did not have the elements in its system, Committee members felt it would be inappropriate to force compliance on the organization.

The Committees discussed “escalating/graduated” or “procedural” penalties. For instance, for the first one or two problems with compliance, data suppliers are not charged a financial penalty. Examples of procedural penalties include limiting access to data for those data suppliers that are out of compliance, and publicly highlighting those data suppliers who are non-compliant.

Neither the Committees nor the Alliance have specific recommendations about the amount of financial penalties. The Alliance, however, would note that if the amount of the financial penalty is relatively insignificant, the data submitter that is out of compliance may determine that non-compliance is a preferred (less expensive) alternative.

**RECOMMENDATION I.2F: Establish a policy and procedure for data supplier resubmission of data.**

Recommendation for Policy and Procedure

Discussion: The lead organization should create a policy within the data submission guide to address circumstances should a data supplier identify errors in their data submission that require resubmissions of data to correct. The Alliance recommends that this be addressed by the lead organization for the APCD and OFM on a case-by-case basis, as it is difficult to anticipate every problem and suggest a resolution.

**RECOMMENDATION I.2G: Create a policy and procedure for exemptions and waivers for mandatory data submitters.**

Recommendation for  
Policy and Procedure

Discussion: The lead organization should create policies and procedures in the Data Submission Guide outlining steps that should be taken when data submitters cannot meet the requirements. This includes such issues as an inability to submit specific data elements or an inability to meet timelines due to major operational problems, like introducing significant new technology. For example, if the data submission specifications required certain data elements be submitted and an organization did not have the elements in its system, Committee members felt it would be inappropriate to force compliance on the organization. In addition, if a health plan implemented an entirely new claims processing system, it may take time for the organization to establish data submissions from the new system to the APCD. As such, the lead organization should establish a policy and procedure for waiver requests, approval and remediation if needed.

**3. VOLUNTARY DATA SUBMISSION REQUIREMENTS**

It is important to understand that self-funded health plans are not mandated to submit claims data to the APCD. However, it is anticipated that some self-funded purchasers (i.e., employers or union trusts) may wish to contribute data or may be directed by their members to contribute data to the APCD on a voluntary basis. This creates a unique challenge for the APCD in that mandated data submissions are made in compliance with the state APCD law, and voluntary data submissions would be made in compliance with Health Insurance Portability and Accountability Act (HIPAA).

Under HIPAA, release of data containing protected health information is generally permitted between a covered entity and a business associate of the covered entity. In this case, a health plan or self-funded purchaser is a covered entity, and an organization performing work on behalf of the covered entity, using data from the covered entity, is a business associate.

HIPAA allows covered entities to release data for three primary purposes: treatment, payment, and health care operations. However, since health plans are required by state law to submit data, they are not doing so for any of these three purposes and, thus, HIPAA is not necessarily applicable. Note: While releases of data by a covered entity are permitted for research purposes, there are other HIPAA provisions covering these uses.

For self-funded plans voluntarily submitting data to the APCD, data must be submitted in compliance with HIPAA. For this reason, appropriate agreements must be established between the various APCD entities (e.g. voluntary data submitter, state, lead organization and/or data vendor) to ensure HIPAA compliance.

It must also be pointed out that the release of data from the APCD will also be affected by the combination of voluntary and mandated data. For example, the APCD law allows for the release of data for a variety purposes. Since the law does not govern those data voluntarily submitted,

covered entities will still need to approve any uses of data they provided to the APCD. This will likely require additional data uses agreements between the lead organization and data requesters, and voluntary data submitters and data requesters.

***As this is a very complex topic, it is highly recommended that appropriate legal expertise be retained to ensure all aspects of compliance, from data submission to release of data from the APCD for reporting and analytic purposes, are covered.***

**RECOMMENDATION I.3A: Permit collection of voluntary data submissions and note that such submissions shall occur under a data sharing agreement/business associate agreement.**

Recommendation for  
Policy and Procedure

Discussion: The lead organization must establish and maintain necessary legal agreements with voluntary data suppliers. Data submissions from organizations that are not mandated and voluntarily submit data will be required to execute a data sharing agreement between the data supplier and the data vendor and/or the lead organization.

**RECOMMENDATION I.3B: Voluntary submitters must use the same formats and standards for submitting data as mandatory submitters.**

Recommendation for  
Policy and Procedure

Discussion: The lead organization should create policies and procedures to ensure that all voluntary data suppliers follow the same data submission technical and procedural requirements as mandatory data suppliers. The Committees and the Alliance noted that in order to efficiently process data, it is important that all data suppliers follow the same data submission technical and procedural requirements.

The lead organization will have limited recourse against voluntary data submitters who fail to meet established timelines and submit data that conforms to minimum standards. Since they are voluntarily submitting data, penalties for non-compliance may not be possible as they are under the state law. It's important that the lead organization already has, or establishes strong relationships with voluntary data suppliers to ensure the data base is enriched by their participation.

#### 4. SECURE COLLECTION/ STORAGE PROCEDURES

Protecting the privacy of individuals and the security of all information in the APCD is of paramount importance to the Alliance and members of both Committees. The lead organization should use related provisions of HIPAA, which sets clear guidelines for how health care data must be treated and stored, as applicable. All aspects of APCD data collection, storage and analysis should meet the highest standards of security and confidentiality.

APCD security features should include constant protection of the data files by overlapping types of security provisions such as encryption, intrusion detection systems, and user access controls. The APCD should also have layers of security that are reinforced through multiple electronic firewalls, controlled access to the physical data center, granting specific levels and types of access permission to users, using a secure website to submit files in an encrypted manner, and emphasizing privacy and security at every point in the data transfer, storage and analysis processes.

For purposes of this section, a data aggregator or data vendor is defined as the entity contracted by the lead organization to manage the intake of data submissions, the aggregation of data submissions into the APCD, and overall operations of the APCD technical infrastructure.

**RECOMMENDATION I.4A: Require the lead organization to create a secure file delivery process for use by data submitters when submitting data files to the data aggregator.**

Recommendation for  
Contract

Discussion: OFM should require the lead organization to use industry standard tools and practices to ensure data security during the data transfer process. The current best practice and recommended approach is to use a Secure Transport File Protocol (SFTP) that is managed by the data aggregator. SFTP is an industry standard file transfer protocol, which allows for the electronic transfer of data in a secure, encrypted manner. The SFTP site requires the data submitter to log on to a secure FTP server and upload files directly to the data aggregator's servers via a secure connection.

**RECOMMENDATION I.4B: Require the lead organization to follow best practices for data encryption and access.**

Recommendation for Contract

Discussion: All sensitive information processed by the APCD should be encrypted and/or de-identified through automatic computer programs, not by individuals. Since it is recommended the submission of data occur over a SFTP connection, data will be encrypted during the data transfer. This is referred to as encryption of data in motion. However, as an added means of protection, it is also recommended that sensitive data (e.g. direct patient identities) also be encrypted while stored in the database. This is known as encryption of data at rest.

De-identified data, or data that cannot be used to identify an individual, may also be encrypted as an extra precaution but it is generally not necessary.

## II. Data Management

### 1. DATA QUALITY

**RECOMMENDATION II.1A: Data quality must be high to ensure credibility, usability and value.**

Recommendation for Policy and Procedure

Discussion: Health care cost and quality will only be improved if the data is of sufficiently high quality that it is credible to those being reported on (for example, doctors, hospitals and payers). The lead organization should create policy and procedures to ensure that submitted data files conform to data specifications and data suppliers demonstrate consistency in the data they submit over time.

To assure provider level reports are of high quality and are credible, it is very important to incorporate data validation into the report process. As claim data is attributed to medical groups, clinics, hospitals using a variety of attribution algorithms, it is important that providers be able to validate the patients attributed to them by the process. This validation process is done by allowing medical groups and hospitals access to a secure website that allows them to review and verify patients attributed to their practices for any report for which they are reported on.

**RECOMMENDATION II.1B: The data submitter and lead organization should check the level of data completeness in data submissions.**

Recommendation for Policy and Procedure

Discussion: The lead organization should create and implement processes to validate data completeness and quality, and share them with the data submitters to foster an environment that invites all stakeholders to be active participants in the quality discussion. The Committees and the Alliance believe that the responsibility for data completeness is shared by both the data submitters and the lead organization. Completeness of data leads to higher quality and credibility of reporting and analytics derived from the database.

As previously stated, it is also important to understand that not all required data may be able to be populated by a given data supplier. In these circumstances, the Committee felt policies and procedures should include allowable exceptions for those cases where a data submitter cannot provide certain data elements because the elements do not exist.

**RECOMMENDATION II.1C: The data quality process and procedure should be defined in policies and procedures, and not rule.**

Recommendation for Policy and Procedure

Discussion: The Alliance recommends that quality processes be maintained in policy and procedure to allow needed changes to be implemented in a timely manner. Quality assurance process improvements, such as the addition of data validation routines for new data fields or the creation of processes to track newly identified data anomalies, often need to happen quickly to address issues as they arise. Having quality processes inserted into rule means that these processes may take up to one year to change, considerably slowing down the quality improvement process.

**RECOMMENDATION II.1D: OFM and lead organization’s contract should consider a number of items related to data submissions and data quality.**

Recommendation for Contract

Discussion: There are a number of items that OFM should require of the lead organization through contract. These include:

- Require an annual report to OFM discussing data validation, data quality and data submitter compliance.
- Develop a short-term, realistic data quality plan to inform the user community about data quality checks the lead organization will initially have in place. Additional quality checks can be developed as needed over time.
- Develop and adopt operating principles to ensure data integrity. The lead organization should demonstrate the quality of the data and communicate this to potential users.
- Produce ongoing, routine statistical testing and standardized reports to promote transparency about data quality strengths and weaknesses.
- Convene a quality-focused Technical Advisory Workgroup. Areas of discussion should include: APCD file specifications, current and future needs; new field edits and intake rules and quality assurance measures; public use files; and reporting tools and reports. The Technical Advisory Group is not a venue for explaining data for analytical purposes; users and analysts should have a separate workgroup.

Massachusetts established a technical advisory committee that is responsible for providing insight about the design and operation of the APCD. In Colorado, the APCD (CIVHC) consults with its APCD Advisory Committee and CIVHC’s Data and Transparency Committee on measurement methodology. These committees are comprised of industry experts who provide discussion and recommendation representing a cross section of industry interests and perspectives.

**2. DATA SECURITY**

The lead organization and data aggregator are responsible for the security of the data once it is transmitted to the data aggregator. Ensuring data is kept and managed securely is of the highest importance. The lead organization and data aggregator must ensure the APCD environment and data stored within are highly secured. This can be accomplished in a number of ways through a variety of tools and technologies. For example data encryption, systems testing and audits, intrusion detection systems, firewalls, creation and adherence to policies and procedures, allowing access to data for only approved uses and users, and restricting data delivery mechanisms (such as not allowing identifiable data to be accessed on the APCD public website).

**RECOMMENDATION II.2A: Create a process and procedure to ensure secure transmission of data.**

Recommendation for Contract

Discussion: OFM should require that transmission of data to third parties (e.g. agencies and researchers) will always be through secure mechanisms. Only the lead organization and data vendor should have direct access to data. Just as with data submissions to the database, data being released from the database should also be transmitted using a Secure Transport File Protocol (SFTP) website that is managed by the data aggregator. SFTP is an industry standard file transfer protocol, which allows for the electronic transfer of data in a secure, encrypted manner. The SFTP site requires the data recipient to log on to a secure FTP server and download the files directly to the servers via a secure connection.

In cases where sensitive or protected data are not being released, it is still advisable to securely transmit data via SFTP or secure email to ensure only the intended party receives the information consistent with any data use agreements that may be in place.

**RECOMMENDATION II.2B: Create a process and procedure to ensure secure storage of data.**

Recommendation for Policy and Procedure

Discussion: The lead organization should create policies and procedures that ensure data in the APCD are securely managed and stored. Given the sensitive nature of data contained in an APCD, it is important to ensure data are securely managed from the initial submission of data into the APCD, through to the delivery of data extracts and reports from the APCD.

The lead organization should not only establish policies and procedures covering secure transmission of data into and out of the APCD, policies and procedures must also be created to define how APCD data should be securely stored within data aggregator's data center or a third party requestor's data environment. This is particularly important for data or extracts containing directly identifiable personal health information. Policies and procedures should take into account such topics as data encryption for data in motion and at rest, access controls to servers and user computers, and access to facilities housing the data infrastructure supporting the APCD.

**RECOMMENDATION II.2C: Convene a Technical Advisory Group to oversee data security.**

Recommendation for  
Contract

Discussion: The lead organization should convene a security focused Technical Advisory Group to provide input into developing and maintaining data security policies and procedures. The group would focus on the technical aspects of data management, such as determining specific encryption processes or access authentication methods, to ensure the environment meets agreed upon security standards.

Membership on this group should include technical representatives from the state, lead organization, data aggregator, data suppliers and others who may have a significant role in management and security of data contained in and released from the APCD.

**RECOMMENDATION II.2D: Develop processes and procedures to mitigate data breaches and to deal with them in the unfortunate event they occur.**

Recommendation for  
Policy and Procedure

Discussion: A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. While HIPAA contains data breach provisions, particularly pertaining to notification responsibilities of covered entities and business associates involved in a breach, data submitted through the state mandate do not necessarily fall under these same provisions as the data are not submitted to the APCD under a normal covered entity / business associate arrangement. The exception is the case in which data are voluntary submitted by self-funded health plans (covered entities) to the data aggregator (business associate).

The committee recommended the APCD lead organization consider addressing data breach in the Data Use or Data Services Agreements. All members agreed this item should be addressed by a formal APCD Data Policy Committee initiated by the lead organization. The Data Policy Committee should consider many factors including, but not limited to, a breach that occurs within the data aggregator's own environment, a breach of the APCD from an external unauthorized source, a breach of data provided to a third party requestor, an inappropriate or unauthorized use of data received by a third party requestor, and a general unauthorized use of data, reports or analysis derived from the APCD.

In all the above cases and others the Data Policy Committee may choose to address, the Data Policy Committee should evaluate and determine the best courses of action in addressing the breach itself. For example, should there be penalties for different types and levels of data breach and/or should entities involved in a breach be restricted from future uses of the APCD.

## Appendix 1: Members of the APCD Data Policy Committee

Committee members were selected from an industry cross section of stakeholders within payer, provider, purchaser, and consumer organizations. Committee members were suggested through existing Alliance members and through other state agency recommendations.

### Data Policy Advisory Membership

First Name	Last Name	Organization	Title/Role
Marc	Baldwin	Office of Financial Management	Assistant Director, Forecasting
Andrew	Behm	Washington Health Alliance	Senior Project Manager
Mary Beth	Brown	Rural Health Clinic Assn	Director of Quality
Bill	Brunkhorst	Pfizer	Senior Account Manager
Mary	Clogston	Consumer Group	Independent Consultant
Patrick	Connor	National Federation of Independent Business (NFIB)	Washington State Director
Nancy	Giunto	Washington Health Alliance	Executive Director
Linda	Green	Freedman Healthcare	Vice President, Programs
Bernie	Inskeep	UnitedHealthcare	Director Regulatory Affairs
Katie	Kolan	Washington State Medical Association	Director of Legislative and Regulatory Affairs
Kathy	Lofy	Washington State Department of Health	State Health Officer
Dave	Marty	Office of Insurance Commission	Chief Information Officer, Operations Division
Lou	McDermott	Health Care Authority	Director, Public Employees Benefits Division
Chris	McGoldrick	Rockwood Clinic	Chief Financial Officer
Sue	Meldazy	Office of Financial Management	Project Director, Health Care Price Transparency Project
Lori	Mitchell	University of Washington	Chief Financial Officer
Cathie	Ott	Health Care Authority, Medicaid	Division Director
Mark	Pregler	Washington Health Alliance	Director, Performance Measurement
Rachel	Quinn	Health Care Authority	Special Assistant for Health Care Policy
Claudia	Sanders	Washington State Hospital Association	Senior Vice President, Policy Development
Kerry	Schaefer	King County	Strategic Planner
Donna	Smith	Western Washington Medical Group	Medical Director
Steve	Swanson	Community Health Plan	Vice President of Information Services & Technology
Molly	Voris	Washington Health Benefit Exchange	Director of Policy

## Appendix 2: Resources

Note: Attached documents and materials are included as illustrative example only. Unless otherwise specified, the contents and format are only for illustrative purposes.

### **ITEM 1**

Agency for Healthcare Research & Quality maintains an inventory of the data elements in APCDs, the United States Health Information Network (USHIK). Users can compare and contrast what each state collects, by file type. The link can be found at <http://ushik.org/mdr/portals/apcd>

A survey of states' data collection best practices and processes was collected by the Arkansas state APCD organization <http://www.achi.net/Content/Documents/ResourceRenderer.ashx?ID=251>

### **ITEM 2**

#### **Data Submission Resources:**

Maine Data Submission Guide: <http://www.maine.gov/sos/cec/rules/90/90/590/590c243.docx>

Colorado Data Submission Guide: This example provides guidance on data submission and includes important completeness threshold for each data element.  
[http://civhc.org/getmedia/c4071074-ecc4-457b-bd40-72fee47ee639/Data-Submission-Guide-V6-March-2014-FINAL\\_1.pdf.aspx](http://civhc.org/getmedia/c4071074-ecc4-457b-bd40-72fee47ee639/Data-Submission-Guide-V6-March-2014-FINAL_1.pdf.aspx)

### **ITEM 3**

#### **Example Data Registration Form**

[http://www.ct.gov/hix/lib/hix/Annual\\_Registration\\_Form\\_20131223.pdf](http://www.ct.gov/hix/lib/hix/Annual_Registration_Form_20131223.pdf)

## Appendix 3: Committee Topics by Month

	September	October	November	December	January
Joint Committee	<ul style="list-style-type: none"> <li>• APCD Overview</li> <li>• WA State Law</li> <li>• Interests and Concerns</li> </ul>				<ul style="list-style-type: none"> <li>• Review Work to Date</li> <li>• Discuss Remaining Issues</li> </ul>
Data Policy	<ul style="list-style-type: none"> <li>• Committee's Role</li> <li>• Data Uses</li> </ul>	<ul style="list-style-type: none"> <li>• Data Collection</li> </ul>	<ul style="list-style-type: none"> <li>• Data Management:</li> <li>• Access Security</li> <li>• Data Quality</li> </ul>	<ul style="list-style-type: none"> <li>• Role of the Lead Organization</li> <li>• Data Fees</li> </ul>	
Data Release	<ul style="list-style-type: none"> <li>• Committee's Role</li> <li>• Privacy Topics</li> </ul>	<ul style="list-style-type: none"> <li>• Data Uses and Users</li> </ul>	<ul style="list-style-type: none"> <li>• Data Access Policy</li> </ul>	<ul style="list-style-type: none"> <li>• Data Release Decision Makers</li> <li>• Accessing Files</li> </ul>	

The development of these recommendations was fully funded (\$50,000) as part of a larger project funded under a Health Insurance Rate Review Cycle III grant from the U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services, Center for Consumer Information and Insurance Oversight awarded to the state of Washington's Office of Financial Management. The total amount of Federal Funds awarded and received by Washington State's Office of Financial Management for the Cycle III grant is \$3,407,553.