



Leading health system improvement

All-Payer Claim Database

Data Release Advisory Committee

SUMMARY OF RECOMMENDATIONS

APCD Data Release 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 members¹ 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

¹ 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 Release 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 major topic area: Data Release and Data Use. 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 Use and Data Release

The Committee's primary concern is to ensure privacy of healthcare information in all circumstances. The Data Release Advisory Committee deliberated on all aspects of data use and data release. The recommendations below focus on key questions about data use and data release such as:

- Who can access the data?
- How may it be accessed?
- How may the data be used?
- What are the legal concerns when releasing data?
- What are the best mechanisms to protect patient privacy and data security?

The goal is to make information from the APCD available to authorized users. The APCD reporting portfolio could include the following options for dissemination and distribution:

- **Reports** through web portals and web applications.
- **Custom reports** through a formal data request and release process.
- **Datasets** that allow specific analysis.
- **Memberships and subscriptions** that provide standard reports, periodically updated, and simple custom views of APCD data.
- **Professional services** that support specific analytic requests as permitted by the APCD's data use standards.

1. DATA USE

RECOMMENDATION I.1A: Develop policies and procedures that encourage use of the APCD data.

Recommendation for
Policy and Procedure

Discussion: The Committees and the Alliance recommend that the state and lead organization create transparent data release processes. The lead organization should consider the following key users and uses when creating policies and procedures:

- Encourage use of the data by general requesters. Use the data for health care policy modeling; trends analysis and benchmarking; assisting informed decision-making; analysis of cost, quality, coverage and access to care; and consumer decision support.
- Encourage use of the data by researchers. While researchers can request data for the same purposes described above, they will also have the ability to request more detailed and identifiable data with approval of an Institutional Review Board (IRB). For this reason, the Committee felt policies and procedures should take into account unique differences in the types of data to be released to different

categories of requestors.

Additionally, the Alliance recommends development of an effective communication plan that describes the data fields available to different users and the process by which they can make requests. This requires a clear understanding about which users have access to which types of data. It also requires the lead organization to have developed the data request and release processes so they can be clearly communicated to potential users.

RECOMMENDATION I.1B: Ensure that safeguards are in place to make sure releases of data are for authorized uses only.

Recommendation for
Policy and Procedure

Discussion: New legislation specifies the level of access and release of data to researchers, government agencies, the lead organization when acting as the lead and when not, other requesters and the general public. The lead organization needs to create appropriate policy and procedures to ensure that the statute is followed for all data requests.

The lead organization should create policies and procedures, including a data request application process, to address circumstances when it is appropriate to release APCD data and for what types of purposes. For example, the Committee felt that APCD data should not be used by an entity for commercial purposes. The policies and procedures should take into account the intent of the APCD described in law.

Following Health Insurance Portability and Accountability Act (HIPAA) law as guidance, Committee members believed that all releases of data should follow “minimum necessary” requirements. This means that data released to a third party should include only the minimum necessary amount of information to meet the needs of the data and/or reporting request.

RECOMMENDATION I.1C: Clearly state prohibition of anti-competitive use.

Recommendation for
Rule

Discussion: OFM should create rule to direct that data is “not to be used for anti-competitive purposes.”

Examples of anti-competitive uses might include: Entities using APCD data to collaborate to set market prices in an attempt to control or prevent competition; a low cost provider using APCD data to evaluate and raise prices to be in line with higher cost providers; using data to create agreements among competitors. The Committee clarified the data may be used to identify geographic areas with a high incidence of a particular condition for the purpose of public health education.

Committee members suggested using Federal Trade Commission anti-competitive guidelines as the basis for establishing rules for the state APCD.

RECOMMENDATION I.1D: Develop a means to address inappropriate data use.

Recommendation for Rule
<p>Discussion: OFM should include definitions of inappropriate data use in rules to assist the Lead Organization and its Data Release Committee in its deliberations. The Committees believed inappropriate data uses should include such things as:</p> <ul style="list-style-type: none">• A prohibition on contacting individuals for any reason.• A prohibition on using information for marketing and/or fundraising to patients.• Re-identification of patients through linking to other information sources unless specifically authorized in the data use agreement.• Re-use of data for “commercial use” by another business. <p>The Committees discussed this last item at length to better define commercial uses that should be explicitly prohibited. One perspective was that an important “commercial” use is to allow a hospital to use the data to determine whether a new service should be developed in a particular area given utilization patterns. On the other hand, there was a lot of discussion about whether data from the APCD should be available for access by for-profit vendors who are creating a new marketable product for sale such as a quality scoring website or APCD data being used by a pharmaceutical company to identify patients using particular drugs and establishing marketing campaigns toward those patients. Payers (health plans) are not in favor of resale of their data to an organization or competitor who would, in turn, profit from the use of the data. Committee members were in agreement with the position of Payers.</p> <p>Inappropriate data uses should be considered further by the lead organization and OFM, and require careful consideration by the Governance Committee as well.</p>

RECOMMENDATION I.1E: Address recourse for misuse of data.

Recommendation for Rule
<p>Discussion: OFM should create rule that clearly outlines misuse of data. Data should be considered misused if it is used for purposes explicitly prohibited by rule, is not consistent with the Data Request Application, is not approved by the Data Release Committee and Lead Organization, and/or is not permitted based on terms of a Data Use Agreement and/or Confidentiality Agreement.</p> <p>In cases where data is determined to have been misused, penalties for misuse should be enforced by the state.</p> <p><i>Note: Legislation passed in 2015 very clearly describes when penalties should be applied for misuse of data.</i></p>

2. DATA RELEASE

RECOMMENDATION I.2A: Develop an efficient and effective data application and release process.

Recommendation for Policy and Procedure

Discussion: The lead organization should create policies and procedures requiring parties interested in receiving ACPD reports or extracts to complete an application that thoroughly documents and considers the organization’s qualifications, prior experience and expertise in managing a project conforming to all applicable federal and state rules regarding appropriate uses of health care claims data.²

Data from the APCD should only be released to organizations that have a well-conceived reason for requesting the data, are requesting it to fulfill the legislative intent of improving health care transparency and are committed to privacy and can demonstrate an operational ability to ensure privacy. In addition, Committee members felt that only the minimum necessary amount of data should be released to fulfill a data request.

RECOMMENDATION I.2B: Develop a thorough Data Request Application form.

Recommendation for Policy and Procedure

Discussion: It is important that uses of ACPD data are consistent with the intent of legislation, that releases of data follow appropriate privacy and security guidelines, and to ensure data are released consistent with APCD policies and procedures. For this reason, the Committee recommends the lead organization create a Data Request Application to provide necessary information to the Data Release Committee, so that they may make informed recommendations to the lead organization for determining an approval or denial of the release of data. The Committee recommended the application include the following minimum details:

- A description and purpose of the proposed project;
- The names and qualifications of individuals who will work on the project;
- The entities that will analyze the requested data;
- A description of the proposed methodology;
- The organization’s experience with similar projects;
- The method of how the data will be stored, returned or destroyed at the conclusion of the project; and
- How the results of the analysis will be used and/or distributed.

Should an application for APCD data be rejected, the Committee also recommended exploring the possibility of having an appeal process. This process would allow a data requestor to gain an understanding of the reasons for rejection, make necessary adjustments to the application, and request another review if desired.

² See Appendix 2, Item 1 for an example of a mature data release process.

RECOMMENDATION I.2C: Ensure Data Application Transparency.

Recommendation for
Policy and Procedure

Discussion: Committee members discussed the need for transparency in how the APCD is being used, including requests for data and reports from the APCD. Some states are placing data requests on a public website so that all interested parties are aware of reporting/data uses. A few of these states even allow for a public comment period on each data request. While the Committee favored the idea of making requests for data and reports public, members felt opening requests for a formal public comment period would be overly burdensome and delay the process for releasing data for valid purposes. Committee members felt that capturing public comments on a website regarding a release could be an option, but the comments should not be a factor in deciding whether to release data or not.

The Committees believe that transparency of use needs to be a basic tenet of state APCD operations and that information about the types of reports being developed will spur the interest of others. The lead organization should create policies requiring all requests of data to be made public.

RECOMMENDATION I.2D: Establish a policy and procedure for timely review of data requests.

Recommendation for
Policy and Procedure

Discussion: The lead organization’s Data Release Committee should create a process to ensure the timely evaluation of data application requests. Recognizing the ability to review and fulfill requests for data or reports from the APCD will largely be dependent on the complexity of the request, availability of resources to fulfill the request, and the number of requests in the queue. Committee members felt requests should be reviewed on a first-in-first-out (FIFO) basis. In addition, committee members discussed an option of using information from previous requests to fulfill new requests if similar in nature and consistent with data release policies.

To also help reduce the time required to respond to data and report requests, Committee members felt the formal Data Release Committee should be comprised of individuals familiar with reporting and analysis using administrative claim data. Having a knowledgeable Data Release Committee can significantly reduce the amount of time required to review requests and make recommendations for release to the lead organization. Committee members also believed the lead organization may be able to make “precedence” based decisions regarding a request without a formal Data Release Committee review in an effort to help expedite the application process.

RECOMMENDATION I.2E: Develop a policy and procedure for public release of provider comparison reports.

Recommendation for
Policy and Procedure

Discussion: The lead organization should consider creating policies and procedures to ensure that applicants are required to submit a copy of the analysis or report to the Data Release Committee or lead organization prior to public release so that any provider comparisons can be validated and reviewed for accuracy. In addition, the Data Release Committee members asserted that including a provider validation step in the data release cycle for reports that include the identification of provider information will help ensure reporting accuracy and build provider trust in the state APCD database. In order to accomplish this, the lead organization and/or third party requestors should provide an opportunity for providers to validate results of any analysis or report for which providers are being compared. This may include the sharing of identifiable patient information with providers to validate the attribution of patients to their practices.

RECOMMENDATION I.2F: Develop Data Use and Confidentiality Agreements.

Recommendation for
Policy and Procedure

Discussion: Data Use Agreements and Confidentiality Agreements are documents signed between the lead organization and a data requester that define the terms and conditions under which access to and use of APCD data is permitted, as well as how the data will be secured and protected by the recipient.

The Alliance recommends that the lead organization create policies and procedures to address the following issues related to data use agreements:

- Define terms and conditions for data disclosure and data use;
- Define terms and conditions of data use between APCD and receiving entity;
- Protect disclosure of direct patient identifiers or re-identification of individuals;
- Establish clarity around eligible data recipients and entities;
- Identify custodian of data at a receiving entity and its accountability;
- Define terms of conditions of data misuse, including penalties; and
- Define data disposal and/or return policies and procedures.

RECOMMENDATION I.2G: Establish a policy and procedure for handling data requests for voluntarily submitted data.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create policy and procedure to ensure third-party requests for access to voluntarily submitted data requires separate permission and data use agreements between voluntary data suppliers and data requestors.

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 employers 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 HIPAA.

For self-funded plans voluntarily submitting data to the APCD, data must be submitted and managed 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 assure HIPAA compliance. Furthermore, each voluntary data submitter must also approve any uses or releases of their data contained in the APCD. For each approved data request, not only do data requestors need to have agreements in place with the lead organization for mandatory data, Data Use Agreements and/or Confidentiality Agreements will also be required between the self-funded entity (voluntary data submitter), the data requestor and the lead organization to ensure proper compliance regarding the release of their data from the APCD.

As an example, suppose the APCD consists of mandated data and data from 12 organizations voluntarily submitting data. A researcher submits a request for data that includes voluntarily submitted data. If the request is approved, each of the 12 organizations would need to independently approve the release of their information to be included in the data release. Separate Data Use Agreements and/or Confidentiality Agreements would be required between each of the voluntary data submitters and the data requestor.

As this is a very complex topic, it is highly recommended that appropriate legal expertise be retained to assure all aspects of compliance from data submission to release of data from the APCD for reporting and analytic purposes are covered. It is also important that voluntary data submitters be fully informed of the potential use of their submitted information by APCD data requestors.

RECOMMENDATION I.2H: Consider the usefulness and practicality of pre-publication reviews.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create policy and procedure that determine whether reports require review prior to publication. Additionally, the policy may allow for data requestors to optionally request report review by the lead organization.

The Committees deliberated the need for pre-publication review to evaluate reporting results for accuracy of calculations and interpretation. There was recognition that there are two inherent side effects of the review function. First, reports that are approved might be perceived to be endorsed by the reviewing body. Second, reports that are not approved could be problematic for the researcher in terms of funding milestones or publication commitments or appear to suppress information from the public.

On balance, the Committees thought mandating a peer view would be administratively cumbersome and that it would be difficult to convene subject experts for the variety of reports that will be generated. The Committees also thought that peer review best occurs in the requester’s “home” organization.

3. DATA ACCESS FEES

RECOMMENDATION I.3A: Establish fees for data access and use.

Recommendation for
Policy and Procedure

Discussion: Current legislation allows the lead organization to establish the data user fees for each type of file.

Pricing for reports and extracts should be comparable and account for relevant differences across requests and uses, and should be inclusive of the true cost to manage and store data. Fees should be based on the cost of doing business, which includes the cost of data storage, tools and the resource cost of producing the report or extract. Data fees must be set by the lead organization.

The committee was not in favor of a tiered pricing structure based on type of applicant, because it would not reflect the true cost of doing business and would disadvantage those with greater resources to pay.

RECOMMENDATION I.3B: Consider a data application fee.

Recommendation for
Policy and Procedure

Discussion: The lead organization should consider creating policies and procedures to require each requestor to complete a short form application that includes a four hour consultation fee. The Policy Committee agreed that this will provide three benefits: a) assists the requestor to understand if the APCD is able to meet their research needs; b) assists the lead organization in understanding the request thus decreasing the likelihood of not meeting the requestor’s expectations; and c) ensures that requests are worthy of consideration as requestors will have an initial financial outlay.

RECOMMENDATION I.3C: Establish clear guidelines for the timing of fee payment by requesters.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create a policy that articulates that payments for reports and extracts should be based on delivery to the agreed upon deliverable requirements. The Committees believe that payments should be tied to the delivery date when the data or file extract is sent to the requestor. A clearly articulated request will help both the requestor and the lead organization understand the terms of service fulfillment.

The Alliance further recommends that requestors pay one-half of the fees for data or reports to the lead organization at the beginning of work and the remaining one-half balance be paid at the conclusion of work. This will minimize the risk of a third party requestor withdrawing their request after the lead organization has put in a significant amount of work to fulfill the request.

RECOMMENDATION I.3D: Create free public access files.

Recommendation
for Rule

Discussion: The OFM rule should direct that files defined and developed for public access should be free of charge.

Data files to be made available for public use would be determined by the lead organization and appropriate committees to ensure the release of data is compliant with the law, rules, and any policies and procedures established for the APCD. The Committee described public access files as highly aggregated (e.g. benchmarks, summary data) datasets. Files should be available for download on a website if possible.

4. PRIVACY AND SECURITY PROTECTION

RECOMMENDATION I.4A: Use existing Federal and State law as guidance for APCD data management and release.

Recommendation for Contract

Discussion: OFM should direct the lead organization to use applicable federal and state law as a guideline to the greatest extent possible for the APCD-specific data release policy.

The Committee discussed using the following HIPAA rules as guidance when considering policies and procedures related to the release of information from the state APCD.

- HIPAA Privacy Rule - *The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.*
- HIPAA Security Rule - *The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.*
- HIPAA Breach Notification Rule - *The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.*

As these HIPAA rules apply primarily to covered entities and business associates, Committee members felt that not all aspects of the rules would be applicable to the APCD. As such they felt requiring full adherence to the rules would be problematic. While all members understood the importance of the HIPAA rules, members felt using the rules as guidance for establishing APCD specific policies and procedures is sufficient.

As little was known about specific state laws during Committee meetings, Committee members recommended the lead organization work closely with state agencies to ensure any applicable state laws are incorporated in the APCD policies and procedures.

RECOMMENDATION I.4B: Develop a policy and procedure for data breach notification.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create data use agreements that include a breach notification policy and procedure. 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 purchasers via their third-party administrators (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 the formal APCD Governing Committee initiated by the future lead organization. The Governing 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 the above cases and others the Governing Committee may choose to address, the Governing 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.

In the event a breach should occur, the policies and procedures should define when it is necessary and under what circumstances individuals with data in the APCD should be notified of the breach. For example, if voluntarily submitted data is breached, voluntary data submitters would need to follow HIPAA notification requirements. However, it was unclear to the Committee if breach notifications are necessary and/or who would be responsible when a breach of mandated data occurs since the data was submitted under state law. While Committee members believed individual notifications would be necessary, members felt more research and discussion was needed to determine how a notification process would be implemented.

RECOMMENDATION I.4C: Develop a policy and procedure for payer and provider data protections.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create policies and procedures that will ensure that provider and health plan identifiers are protected. This should be accomplished primarily through the Data Release Committee’s analysis of data request application forms. In addition, legislation passed in 2015 clearly defines Proprietary Financial Information in a way that prohibits releasing provider and payer information that reveals the specific contract arrangements between payers and providers.

The Committee discussed provider identifiers that are often the Social Security Number or Federal Tax Identification Number of the provider. These elements should be protected just as individual patient identifiers are protected. All sensitive identifiers should be encrypted or replaced with obfuscated identifiers while still maintaining the uniqueness of the information they represent.

Examples of existing APCD’s policies addressing provider and payer protections fall on all points of the spectrum. For example, New Hampshire and Maine allow open access to provider and payer information. On the other end, Minnesota prohibits release of any provider or payer identifying information. In the middle, is the CMS Qualified Entity program, which allows for release of provider specific information with the provision that providers have an opportunity to verify and make corrections before publication.

RECOMMENDATION I.4D: Develop policies and procedures that provide privacy protection of the data.

Recommendation for
Policy and Procedure

Discussion: The lead organization should create processes, policies and procedures to allow for data release and data use in a manner that provides for data security and individual privacy of information. The primary APCD privacy and security procedures to be developed in conjunction with the recommendations of the Data Policy Committee should be the basis for developing privacy and security procedures for data use and data release. By building upon the core APCD privacy and security policies and procedures, the data release policies and procedures will focus strictly on those core requirements related to release and use of data. It is recommended that data release policies and procedures extend to any third party requestor taking receipt of APCD data to ensure consistency in the management and security of sensitive information.

Appendix 1: Members of the APCD Data Release 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 Release Committee Membership

First Name	Last Name	Organization	Title/Role
Marc	Baldwin	Office of Financial Management	Assistant Director, Forecasting
Carolyn	Barton	Group Health	Chief Compliance and Ethics Officer
Andrew	Behm	Washington Health Alliance	Senior Project Manager
Jonathan	Bennett	Washington State Hospital Association	Director of Decision Support
Joe	Campo	Office of Financial Management	Senior Forecast Analyst
Doug	Conrad	University of Washington	Professor, Health Services
Bev	Court	DSHS	Epidemiologist
Nancy	Giunto	Washington Health Alliance	Executive Director
Linda	Green	Freedman Healthcare	Vice President, Programs
Bernie	Inskeep	UnitedHealthcare	Director, Regulatory Affairs
Jessie	Matt	Group Health	Senior Counsel and Group Health
Sue	Meldazy	Office of Financial Management	Project Director, Health Care Price Transparency Project
Bob	Perna	Washington State Medical Association	Director of Health Care Economics
Mark	Pregler	Washington Health Alliance	Director, Performance Measurement
Brian	Ritchie	Regence BlueShield	Assistant Director Actuarial
T. Howard	Stone	DSHS	IRB and Human Protections Administrator
Catherine	Walberg	Physicians Insurance	Senior Vice President, General Counsel
Brandon	Wong	Washington State Hospital Association	Senior Analyst II, Decision Support

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

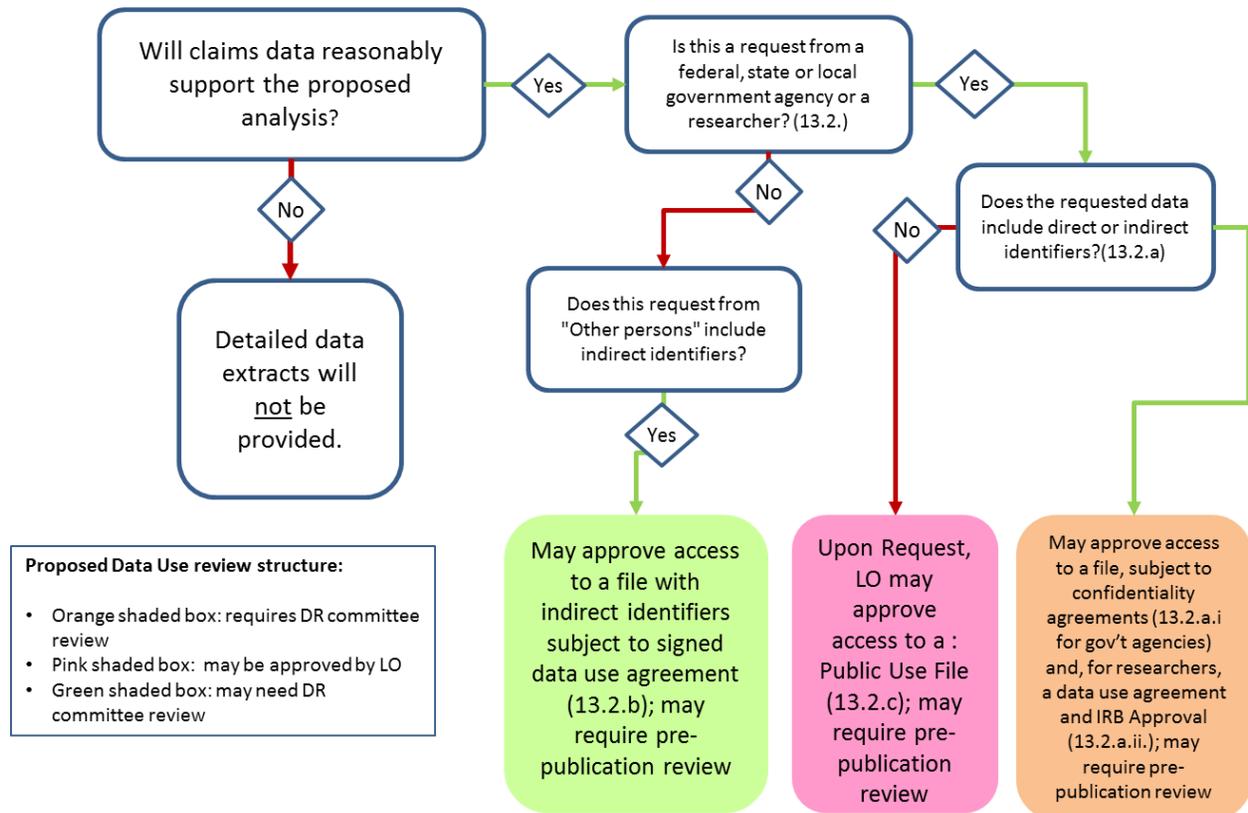
Data Release Resources

CIVHC Data Request/ Release Page: <http://www.civhc.org/All-Payer-Claims-Database/Data-Release-Review-Committee.aspx/>

Appendix 3: Committee Topics by Month

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

Appendix 4: Data Release Workflow Model as recommended by the Alliance and APCD Committees based on 2014 Legislation



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.