

Kentucky Health Data Trust Initiative

APCD Data Governance – Best Practices and Lessons Learned

Deliverables 4.1.1 and 4.2.1

Prepared for the Kentucky Health Data Trust
Interagency Governance Workgroup

Freedman HealthCare
June 29, 2015



INTRODUCTION

Successful All Payer Claims Databases (APCDs) around the country use a range of data governance models to ensure that the goals of the project are met during all phases of the project. In practice, governance is a framework that combines legal, operational and public engagement requirements in three key areas: **data collection**, **data quality**, and **data access**. For each, a state's APCD team must define policies, establish guidelines, and designate responsibility. This brief discusses key data governance considerations for each area, and presents best practices and lessons learned from other states. This discussion does not include oversight of the data systems and infrastructure used to actually store the files. Those conditions will be addressed in the System Feasibility Assessment series of deliverables.

BEST PRACTICES FOR BUILDING A DATA GOVERNANCE STRUCTURE

Define a strong Statement of Purpose: Health system stakeholders have the most concerns about how an APCD will be used. While the “early adopter” states (ME, NH, VT) were able to overcome opposition early on, more recent APCDs have encountered greater resistance. For example, stakeholders in other states express concerns that the data require full review before the APCD can release detailed price and quality data. In response, APCDs create Reporting Plans that show a thoughtful progression from aggregated, geographic public policy information towards more detailed, granular reporting. The Reporting Plan describes the different types of analyses and files that will be available to the public, state agencies, researchers and other users. This Plan sets a tone of public communication and offers a schedule for when data will be ready for review, a plan for ongoing stakeholder engagement, and a high level timeline. States that wish to implement an APCD should begin the dialogue early with data submitters and providers to develop a shared understanding of what will be reported. APCD leaders will revise the Reporting Plan as timelines become more concrete and state policy needs emerge.

Examples of Reporting Plans

- Colorado: [2011 Report to the CO legislature](#)
- Connecticut: [2013 APCD Advisory Group quarterly meeting](#)
- Rhode Island: See [Appendix 1](#)

Armed with a vision for the purpose and the uses of the APCD, the governance structure can move forward to address key aspects of governance. The components subject to external input include defining the data collection process, monitoring the quality of the database, and providing access to qualified users through a variety of distribution models.

Establish a Stakeholder Advisory Committee: In keeping with transparency and the ongoing need for community support, states should appoint a multi-stakeholder Advisory Committee to provide ongoing input and insight into the plans for the APCD (see [Appendix 2](#) for a list of the entities that are typically represented in these Committees). Many mandatory APCD states include provisions for a governor-appointed board that meets periodically to weigh in on the implementation and operation of the APCD. Having this forum drives regular reporting, provides early warning about issues of concern, and builds a constituency for broad access to reports and analytic services. Some of the principles that have emerged from APCD advisory groups tasked with defining the APCD reporting process include the following:

- *Create realistic, phased in timelines*
- *Select what is to be measured in collaboration with prospective users*
- *Define what decisions the data will influence*
- *Show meaningful variation (do not exaggerate differences to drive comparisons)*

- *Establish a clear methodology for measurement, using nationally accredited standards when appropriate*

With input and guidance from the Advisory Committee, states must clearly define the data governance framework around data collection, quality, and access, as described in more detail below.

LESSONS LEARNED FOR A DATA GOVERNANCE FRAMEWORK

A. DATA COLLECTION

The first component of the data governance framework is defining what data will be collected, how the data will be collected, and who is responsible for providing the data.

1. Determine what data are needed to meet the Reporting Plan's vision

An APCD requires a data submission guide that clearly defines the data submission requirements needed to standardize inputs. Files that are not normalized to a single standard require transformations that may inadvertently misrepresent the data. A common definition for submitted data supports more streamlined data processing and analysis. In addition to creating a format for data submission, the APCD must establish policies and procedures for:

- Collecting data monthly or quarterly to speed up the timeliness of reports
- Filing exemptions for submitters with covered lives below a particular threshold, which ranges from 1,000 to 5,000 covered lives depending upon the size of the state and the number of submitters
- Filing exemptions for certain categories of coverage, such as accident and disability only plans, auto insurance, long term care and Medicare Supplemental insurance (Medigap) plans
- Granting waivers or variances from the data submission guide standards

This data submission guide provides a standard to which all submitters are accountable, and allows the APCD data team to more easily check incoming data files to confirm that they include all required fields.

2. Determine the legal basis for data submission

Generally, states use three distinct models to collect claims data from commercial carriers: mandated by state law, voluntary under HIPAA, or pursuant to contract terms and conditions. [Appendix 3](#) compares and contrasts the different models.

Mandatory data submission

To date, eighteen states have passed APCD legislation, which allows health insurance companies to provide copies of their files under the HIPAA public health exemption and eliminates the need for data use agreements. APCD laws usually designate a state agency to assume responsibility for issuing rules that govern the details of data submission, such as formats, timelines and penalties. State practice varies on the level of detail about data submission within the rule itself. Some incorporate the submission guide into the body of the rule itself, some incorporate by reference, and some allow the responsible state agency to issue technical guidance as needed. In any scenario, state regulators should limit changes to once per year and provide at least four months for data submitters to come into compliance with the revised requirements.

Voluntary filings

Under a voluntary arrangement, the APCD team creates a standard Data Use Agreement that describes the requested data collection, data management strategies and proposed data uses. Ideally each data submitter agrees to all the terms and conditions in the standard DUA. HIPAA allows data disclosure for research purposes, which may or may not align with state policy goals. Achieving agreement on voluntary Data Use Agreements typically requires 12 to 24 months of effort.

Similar to states with APCD laws, states using a voluntary data submission model should clearly define their data submission guidelines. Without legislative authority, states may find it difficult to enforce data submission standards, and key data elements may be unavailable. Therefore, the data from voluntary submissions may be more useful for understanding certain aspects of health care service delivery more than others. State-wide APCDs are generally mandatory so there are fewer lessons learned for voluntary agreements.

Other methods

States can pursue other means of gathering commercial claims data without a legislative mandate by building APCD data submissions into the terms and conditions of carriers' state contracts. For example, a state could require commercial carriers that wish to participate in the state employee benefits program to submit data for their complete book of business in that state, as a condition of participation. In addition, the Centers for Medicare and Medicaid Services' revised rules for Medicaid Managed Care Organizations (released in May 2015) include more robust requirements for data submission; therefore, states might consider requiring that commercial carriers submit data for their commercial member population as a condition of being a Medicaid MCO. Finally, some states under health care reform have required health plans serving subsidized individuals to submit claims data for those populations. States aiming to build a voluntary data submission model should explore alternate means of gathering claims data.

Data Use Agreement Provisions that Facilitate Sign-On from Voluntary Submitters

- a. Payer submissions contain only de-identified data.
- b. Payer submissions contain no price information (only charges).
- c. Payer is not identified in any reports, and all reports conform to FTC Safe Harbor guidelines.
- d. The uses and activities conform to HIPAA Privacy and Security Rule.
- e. Reports and uses are clearly defined; no other uses are permitted without specific permission.
- f. Describes which state agencies may have access to the data and through what mechanism access will occur.
- g. There are no "data use fees" or data monetization.
- h. Submission guidelines use standard formats and respect the limits of claims payment systems.

B. DATA QUALITY

The second key component of data governance is building systems and processes to ensure that the submitted data are reliable, valid, and of good quality. There are three main phases of data quality assurance that APCD teams must implement. As part of the data governance planning process, states should build protocols and identify the responsible parties for each phase.

Phase 1: Create data collection standards

All APCDs check data when the files are initially collected from carriers, requesting resubmissions from carriers to correct identified errors, and documenting when submitters do not meet minimum data specifications.

Phase 2: Examine the production files for consistency

Once the data have passed the series of initial checks against standards, the APCD team runs checks for internal consistency and completeness over time. In addition, the team should check to confirm that every member on a claim file can be linked to a corresponding member record, and that member data

are consistent from month to month. The team can also check for discrepancies in the data, such as sharp spikes in enrollment or claims activity, or missing zip codes.

Phase 3: Analyze the data

The APCD team should conduct further quality analyses once the data are in a data warehouse with business intelligence (BI tool). Production files can use value-adds for additional quality checking – for example, using a risk assessment or illness burden tool to examine the persistence of diagnoses and conditions at the member level over time. This phase should conclude with summary reports to data submitters to confirm that APCD data align with their records.

More information on key lessons learned related to data quality can be found in **FHC Deliverable 5.3 – Lessons Learned for APCD Infrastructure**.

C. DATA ACCESS

The final component of the data governance framework is data access. The primary concern of many stakeholders is usually “How will my data be used?” Data submitters may be hesitant to relinquish any data if they fear it will be poorly safeguarded, misused, or misinterpreted. Therefore, states must build a robust governance structure to define data policies, oversee data release, and validate data findings prior to publication. While the makeup of this governance structure may look slightly different state by state, most APCDs typically include the following data governance components:

Data Release Policy Development

Either the Advisory Committee (described above) or a separate group of experts should be responsible for framing policies for data access and use. In some states, the Advisory Committee establishes high-level policies and requirements that will become the framework for data use, and a separate Data Release Committee makes recommendations on specific requests. In developing policies, these groups consider the following issues:

- The individuals or entities that will have access to the data, and for what purpose (there may be several levels of access)
- The means of access (e.g. custom reports, data extracts, data enclaves; these may differ based on the level of access)
- The level of detail that can be publicly reported; for example:
 - Whether provider names will be published, and the necessary conditions for this
 - Whether payers will be compared to each other by name, and for what purpose
 - Whether this information should be available for internal audiences only, or also for health care consumers and other external groups
- The process for validating APCD data and findings prior to releasing a report
- The individuals or entities who must be notified prior to releasing the data in a public-facing report or publication

Case-by-Case Review Board

Some states charge the Data Release Committee with reviewing all requests for APCD data from external entities such as academic researchers or other groups. In other states, the Data Release Committee appoints a sub-committee to review case-by-case applications. In this model, external entities (e.g. academic researchers or other groups) that wish to access APCD data may apply for a data extract, citing why they need the data, what data elements they need, how it will be used, and if/how the findings from the analysis will be disseminated. A Case-by-Case Review Board reviews these

applications and determines if the request is aligned with the policies established by the Advisory Committee.

It is the responsibility of the Review Board to ensure data privacy and prevent the unnecessary release of protected health information or other data guarded by HIPAA. As such, the Review Board should include data privacy experts both internal and external to state government, who will determine that all data releases present a minimal risk to disclosing the identity of any individual. The Review Board usually requires that external data requesters receive IRB approval for their research project prior to submitting their application to the APCD Review Board. This helps flag and deter any studies that the IRB classifies as human subjects research.

When approving a request for a data extract, the Review Board will execute a data use agreement (DUA) with the applicant. The DUA should include clear language that defines how the data will be accessed, stored, and released. The DUA should also prohibit any attempts by the researcher to re-identify individuals, and should clearly specify the researcher's ability and/or plans to link the data to other data sets.

Technical Review Board

Some states also establish a Technical Review Board as a sub-group within the Data Release Committee. The purpose of this group is to evaluate and review any APCD information or analyses prior to publication or release. This ensures that the final product is aligned with the original data application, and can also verify that conclusions are reasonable and evidence-based.

At this time, only seven APCD states are actively releasing any data (ME, NH, OR, CO, MA, UT, and VT) from the APCD. Three (MA, ME and UT) have formal committees that may be convened to review the reports based on APCD data. In some cases, the Technical Review Board simply reviews draft publications to confirm that the researcher has used the data for the purposes originally proposed. Other states are more concerned that the data will be misinterpreted, and have implemented additional review processes to validate the research findings.

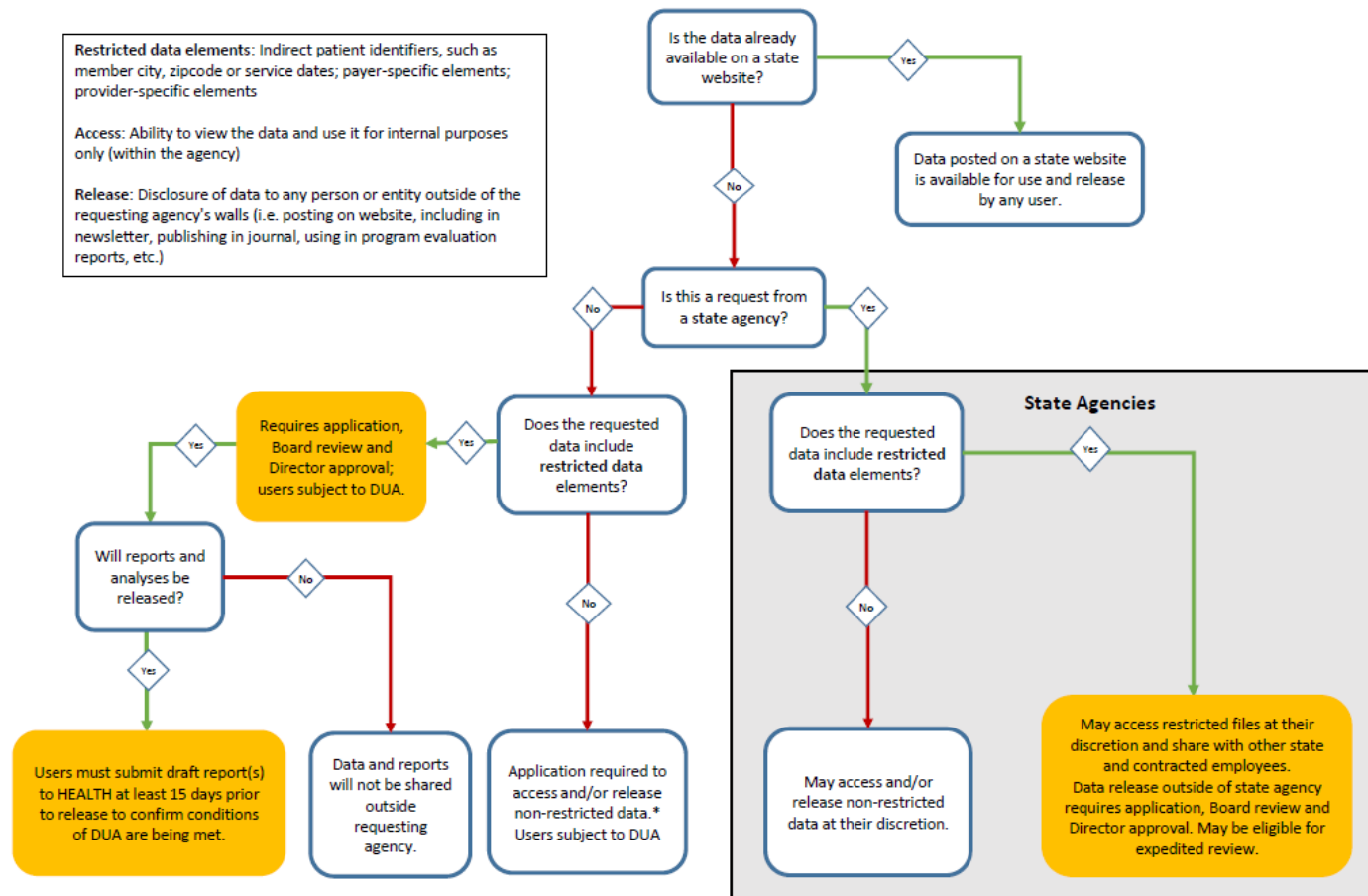
There are various models that states use to oversee data access. When building the data governance structures for an APCD, states must determine the model that best fits the state's vision, resources, and needs. For an example of how a state structures its data release policies, see [Appendix 1](#).

For an example of how the data governance framework is structured in a fully operational APCD, see [Appendix 4](#).

Additional lessons learned for APCD data quality, use, and release can be found in the following brief, developed by Freedman HealthCare and published by the Robert Wood Johnson Foundation: [Realizing the Potential of All-Payer Claims Databases: Creating the Reporting Plan](#).

APPENDIX 1: Example Data Release Process*

Rhode Island APCD - Data Release Flow Chart



*Applications will be reviewed to ensure that no restricted data elements are requested.

Yellow shaded boxes = Requires Data Release Review Board review and HEALTH approval in order to move to next step in process.

*Note: This is a draft public document; therefore, the data release process may be modified slightly.

APPENDIX 2: Summary of Advisory Committee Members

	Colorado	Washington	Arkansas	Connecticut
APCD Administrator				✓
State Agency or Payer	✓	✓	✓	✓
Academic researchers	✓		✓	
Health Care Providers/ Practitioners	✓	✓	✓	✓
Nonprofit data quality organization	✓			
Commercial Health Plans	✓	✓	✓	✓
Consumers	✓	✓	✓	✓
Other	✓		✓	

APPENDIX 3: COMPARISON OF MANDATORY, VOLUNTARY, AND CONTRACTUAL DATA USE

	Mandatory	Voluntary	Other
Example	State APCDs in Utah, CT, CO, ME, NH, etc.	Virginia (statewide by law)	State employee plans must submit entire book of business to get state contract
Legal Authority	State law	HIPAA Research Provisions	HIPAA Business Associate Agreement
Governing Documents	State law and rule	Data Use Agreements	Business Associate Agreement
Data submission	As permitted under law	As permitted by HIPAA (usually a Limited Dataset)	As dictated by contract terms
Quality	State may dictate and enforce standards; require corrections	State may request error corrections	As dictated by contract terms
Uses	As envisioned in state law (usually broad)	Limited to uses in the Data Use Agreement	As dictated by contract terms, usually specific to contract administration
Formal Access Review and Approval	Usually a legislatively mandated Data Release Committee to assess alignment with state goals and privacy protection	Each data submitter reviews and approves a new use	Per contract
HIPAA	State law creates exemption for state data submitters; may mimic HIPAA; Medicare data from CMS is subject to HIPAA	All uses and types of data, reporting and analysis are subject to HIPAA (e.g.	Subject to HIPAA reporting rules

APPENDIX 4: Example Data Governance Structure

Figure 1 is an illustration of the governance model for the Colorado All Payer Claims Database. The Colorado Governor and Legislature designated the Department of Health Care Policy and Financing as the state agency with regulatory authority to select and oversee the work of the APCD Administrator through rule, reporting and appointment of Advisory Committee members. The nonprofit Center for Value in Health Care (CIVHC) reports to its Board of Directors and Data and Transparency Committees. CIVHC consults with the governor-appointed Advisory Committee on policy matters. By rule and process, CIVHC convenes a data release review committee to set data access policy and consider specific requests for access and reports.

Figure 1: Colorado APCD Governance

Appendix F: APCD Oversight Roles and Relationship

