Colorado All Payer Claims Database
Privacy, Security and Data Release Fact Guide

CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

All Payer Claims Database: Background

The Colorado All Payer Claims Database (APCD) collects health insurance claims from public and private payers into a secure database. Created by legislation in 2010 and administered by the Center for Improving Value in Health Care (CIVHC), the APCD is Colorado's most comprehensive source for information about health care spending and utilization in Colorado. As of January 2013, the APCD includes health insurance claims from Medicaid and the eight largest health plans for the individual and large group fully-insured markets. These claims represent more than 2.5 million Colorado residents, or over 50 percent of the insured population in the state. By the end of 2014, the APCD is projected to include claims information for remaining segments of the commercial market as well as Medicare, eventually reflecting the vast majority of insured Coloradans.

APCD Security and Data Availability: Summary

In accordance with Department of Health Care Policy and Finance (HCPF) rules (10 CCR 2505-5-1.200.5), CIVHC is required to ensure the APCD follows all HIPAA privacy and security regulations to protect patient information. Claims information in the APCD is encrypted, both in transmission and while stored, and resides on secure servers which undergo systematic ongoing testing for security. Only high-level aggregated information is available on the public APCD website (www.cohealthdata.org); **no** individual or personal information may be seen on the APCD site.

Limited and controlled release of APCD data is allowable under the established HCPF rules, provided Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules are strictly enforced and the purpose of the data request meets the goals of the Triple Aim for Colorado: better health, better care and lower costs. The rules require that a multi-stakeholder Data Release Review Committee (DRRC) review data requests and advise the Administrator whether such requests meet these criteria and will contribute to better health for Coloradans.

APCD Security and Data Availability: Detailed Q&A

Who decides who can get information from the APCD? What rules do they use?

The APCD governance rules promulgated by HCPF require that the DRRC develop protocols for the release of APCD data. The DRRC comprises health care data and analytical experts representing a variety of organizations and stakeholder perspectives. The rules require that the DRRC shall review the request and advise the Administrator on whether release of the data is consistent with the statutory purpose of the APCD, will contribute to efforts to improve health care for Colorado residents, complies with the requirements of HIPAA and will employ appropriate analytical methods. Requests must meet all these criteria in order to be approved. Approved data requests then require the requestor to enter into a very strict Data Use Agreement. Additionally, the APCD Administrator is required to report annually to HCPF listing data requests, their use and how they met HIPAA requirements.

What kind of information can organizations get from the APCD?
By rule, the APCD Administrator is permitted to provide or "release" data at varying levels of detail and specificity. All releases of APCD data must meet all HIPAA privacy and security guidelines and are subject to review and advisement from the DRRC, which requires that the intended use supports reaching the Colorado Triple Aim of better health, better care, and lower costs. For example, public and private entities may request information on costs associated with treatment of a specific diagnosis or disease by region or county, variation in cost of procedures by facilities, and utilization of high cost services such as MRIs for a defined population.

Are there limitations on the data that organizations can get from the APCD?
Yes, APCD data releases are subject to both HIPAA restrictions and state legal and regulatory restrictions to protect privacy:

1. In keeping with the "minimum necessary" standard established under HIPAA, applicants must demonstrate need and provide justification for each data element requested. The DRRC will recommend and the APCD Administrator will release only those data elements which are specifically necessary to accomplish the applicant's intended use.
2. Protected Health Information (PHI) may only be released in limited circumstances for public health, health care operations and pre-approved research purposes, and can never be shared publicly as a result of a research project or program.
3. For research-related requests, applicants may be required to show written approval from an Institutional Review Board or a Privacy Board as part of the Application.
4. As part of the Data Use Agreement, all Applicants must provide written assurances that:
    - Data will be used only for the purpose stated in the Application.
    - No attempt will be made to use any data supplied to ascertain the identity of specific insured individuals or patients, or to report data at a level of detail that could permit a reader to ascertain the identify of specific insured individuals or patients, nor will downstream linkages to outside data sources occur without specific authorization from the APCD Administrator.
    - Restricted data elements such as PHI will not be released except as specifically approved in the original Application and Data Use Agreement.
    - The Applicant will obtain these assurances in writing from any recipient of data or agent that processes data on behalf of the Applicant.
    - The data will not be re-released in any format to anyone except personnel identified and approved in the original Application and Data Use Agreement.

What information is required in order to submit a data request?
According to both APCD statute and HCPF rules, all data release applications must be submitted in writing and describe in detail:

- The purpose of the project and intended use of the data.
- Methodologies to be employed.
- Type of data and specific data elements requested along with justification.
- Qualifications of the research entity requesting the data.
- The specific Privacy and Security measures that will be employed to protect the data.
- Description of how the results will be used, disseminated or published.

The DRRC reviews the data release applications and advises the Administrator on approval or denial.

What kind of organizations can get information from the APCD?
Both public and private entities may receive APCD reports subject to review and advisement of the request by the DRRC. Organizations that have requested information from the APCD so far include university researchers, divisions of Colorado state government and private firms developing new pricing models for health care services.

What can APCD data be used for? Are there any restrictions on the purposes for which it may be used?
Data requests may only be used to inform projects or support programs that support the achievement of one or more of the categories of the Triple Aim for Colorado: better population health, better quality of care and patient experience, and lower cost of health care. Data cannot be used to directly market to individuals for market gain of an individual or organization. For example, a data request identifying all diabetic patients for purposes of target marketing a new diabetic drug does not meet the intended use criteria. Personal health information can never be shared publicly as a result of a research project or program.

Can an organization charge others for information it gets from the APCD?
Under an approved request, use of the released data is limited to the specific purpose as described in the original application. Further use of the data for a purpose not reflected in the original application would require a new request that fully complies with the privacy and security requirements of HIPAA.

Is there any circumstance in which a private company or individual could get personal, identifiable health information out of the APCD?
HIPAA allows the release of certain, limited data fields for very narrow purposes: public health activity, health care operations, and research activity. The DRRC will review every request for APCD data reports to ensure that no information is released that goes beyond HIPAA rules and the Administrator will deny any request for data or reports that would violate HIPAA or state law and rule.

Could a company get a report from the APCD identifying all the people in a given zip code who have a certain diagnosis or have been prescribed a certain drug?
There is no circumstance we can envision in which a company could obtain this data without first directly obtaining patient authorization to do so. The company would then have to meet all other data release requirements including showing how this information would improve health, care or lower costs. Similar to HIPAA laws that govern providers or payers, release of specific names of patients can only occur in the most unusual public health circumstances or under research protocols that under HIPAA laws require patient authorization or Institutional Review Board research approval.

What happens if an entity misuses APCD data or uses it for a purpose other than that for which the entity applied?
An approved applicant must sign and enter into a Data Use Agreement or contract with the APCD Administrator and agree to the following:

- Restrictions on data disclosure and prohibitions on re-release of the data.
- Prior approval from the APCD Administrator subject to DRRC guidelines is required to publicly release any reports based on the data. The APCD Administrator will carefully review all materials intended for publication or dissemination to determine whether the privacy rights of any individual would be violated by the release of the information.
- Violation of the terms of the Data Use Agreement constitutes a breach of contract and may:
  a. Require the immediate surrender and return of all APCD data.
  b. Result in denial of future access to APCD data.
  c. Lead to civil action by the Administrator for breach of contract.

d. Result in a complaint filed with the U. S. Department of Health & Human Services, Office for Civil Rights, as well as civil and criminal action and penalties.
e. State Attorneys General are also empowered under the HITECH Act to take civil action regarding certain HIPAA violations.

How is the APCD Administrator held accountable for the use of APCD data?
The APCD Administrator is required to provide HCPF with an annual report on or before April 1 of each year that includes:

1. Any policies established or revised pursuant to state and federal medical privacy laws, including HIPAA.
2. The number of requests for data and reports from the APCD, whether the request was by a state agency or private entity, the purpose of the project, a list of the requests for which the DRRC advised the Administrator that the release was consistent with rule and HIPAA, and a list of the requests not approved.
3. For each request approved, the Administrator must provide the HIPAA regulation pursuant to which the use or disclosure was approved, and whether a data use agreement or limited data set data use agreement was executed for the use or disclosure.
4. A description of any data breaches, actions taken to provide notifications, if applicable, and actions taken to prevent a recurrence.

How do you protect the information in the APCD?
The safety and privacy of personal information is a foundational principle of how the Colorado APCD is designed and operated. Not only is data encrypted and protected but personal information will never appear in any public APCD data output or report.

Data Security: When carriers submit files to the APCD, the datasets are always encrypted and sent over a secure connection to Treo Solutions, the APCD Data Manager. This connection is limited to a pre-determined list of users and IP addresses (internet connections) reserved for the carriers submitting the data. The servers holding APCD data are "hardened" to prevent downloading data to a laptop, USB drive, disc or other device. It is not possible to get remote access to the APCD (e.g., from a Treo employee's home computer). Further, Treo Solutions conducts quarterly "penetration" (hacker) testing of the APCD to detect potential areas of vulnerability.

Elimination of personal identifiers: As data are loaded into the warehouse, all personal information is automatically removed from the record and replaced with a separate, unique identification number that does not incorporate any personal information. Additionally, birth date is replaced with age category and zip codes are reduced to the first 3 digits (or 000 if from a zip code with fewer than 20,000 people).

Controls on how the database is used for analysis and research: Simply stated: your personal information will never appear in any public APCD data output or report. All requests for APCD data must detail the purpose of the project, the methodology, the qualifications of the research entity and, by executing a data use agreement, comply with the requirements of HIPAA. The DRRC reviews the request and advises the Administrator whether release of the data is consistent with the statutory purpose of the APCD, contributes to efforts to improve health care for Colorado residents and complies with the requirements of HIPAA.

What would a hacker see if he got into the database?
Encrypted information as illustrated above. All information in the APCD is encrypted during transmission from the health plans and while it is "at rest" in the database. To mitigate encryption key compromise, each submitter is identified prior to submission by Internet protocol (IP) address. These IP addresses are unique, and transmission is only allowed from these sources. Additionally, each submitter is provided with a unique encryption key, which encrypts the data while in transit. Once the data is decrypted and processed, the source data at rest is encrypted using advanced encryption standard (AES 256 bit) and protected.

Could an employer or a law enforcement agency requisition information about an individual from the APCD?
Based on the APCD statute and HCPF rules, the APCD must adhere to federal privacy laws, specifically HIPAA, regarding data disclosures, just as your insurance company must do with respect to claims information. The APCD statute and rules provide no special protection from law enforcement, and there are HIPAA exceptions that, under some circumstances, allow for data disclosures (e.g., certain law enforcement purposes, certain judicial proceedings). Any data that was released under such circumstances would, however, require that HIPAA's privacy standards be met.

Data Release Review Committee Members

Name	Title & Organization	Representation
Jonathan Mathieu	Director of Data & Research, CIVHC	Committee Chair
Alma Jackson	Associate Professor, Loretto Heights School of Nursing, Regis University	Non-Physician Provider
Scott Anderson	Vice President, Professional Activities, Colorado Hospital Association	Hospital
Ako Quammie	Director of Information Systems, Integrated Physicians Network	Physician Provider
Mark Miller	Kaiser Permanente	Payer (nonprofit)
Matthew Frankel	Anthem/Wellpoint	Payer
Rene Horton	Business Analysis Section Manager, CO Department of Health Care Policy and Financing	Public Payer
Nathan Wilkes	Owner/Principal Consultant, Headstorms, Inc.	Additional Perspective
Bob Semro	Health Policy Analyst, The Bell Policy Center	Additional Perspective
Amy Downs	Senior Director for Policy and Analysis, Colorado Health Institute	Additional Perspective
Kavita Nair	Associate Professor, Pharmaceutical Sciences Program, University of Colorado	Additional Perspective

APCD Oversight Roles and Relationships