

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



## **Colorado All Payer Claims Database: Background**

The Colorado All Payer Claims Database (APCD) collects health insurance claims from public and private payers into a HIPAA and HITECH compliant secure database. Created by legislation in 2010 and administered by the Center for Improving Value in Health Care (CIVHC), the CO APCD is Colorado's most comprehensive source for information about health care spending and utilization in Colorado. As of March 2016, the CO APCD includes health insurance claims from Medicaid, Medicare, Medicare Advantage, and the 33 largest commercial health plans for the individual, small group and large group fully-insured markets. These claims represent more than 3.5 million Colorado residents, and over 65 percent of the insured population in the state. The CO APCD is continually enhanced and is projected to eventually include claims reflecting the vast majority of insured Coloradans.

## **CO 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 CO APCD follows all HIPAA privacy and security regulations to protect patient information. Claims information submitted to the CO 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 CO APCD website ([www.comedprice.org](http://www.comedprice.org)); **no** individual or personal information may be seen on the CO APCD site.

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

## **CO APCD Security and Data Availability: Detailed Q&A**

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

The CO APCD governance rules promulgated by HCPF require that the DRRC develop protocols for the release of CO 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 CO 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 recommended for approval. Once approved, APCD rules

require the requestor to enter into a HIPAA compliant Data Use Agreement. Additionally, the CO APCD Administrator is required to report annually to HCPF listing data requests, their use and how they met HIPAA requirements. A summary of approved data requests is also included in the annual report to the Governor and General Assembly.

### **What kind of information can organizations get from the CO APCD?**

By rule, the CO APCD Administrator (CIVHC) is permitted to provide or “release” data at varying levels of detail and specificity. All releases of CO APCD data must meet all HIPAA privacy and security requirements and are subject to review and recommendation for approval by 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 CO APCD?**

Yes, CO APCD data releases are subject to both HIPAA and state legal and regulatory requirements to protect patient privacy and ensure data security:

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 CO APCD Administrator will release only those data elements which are absolutely necessary to accomplish the applicant's intended purpose.
2. Protected Health Information (PHI) may only be released in limited circumstances to support public health, health care operations and research purposes as defined under HIPAA, and can never be shared publicly as a result of a research project or program.
3. For requests that include PHI, researchers are 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 DRRC recommendation for approval and specific authorization from the CO APCD Administrator.
  - Restricted data elements such as PHI will not be released except as specifically approved in the original Application and Data Use Agreement and in full compliance with HIPAA standards.
  - 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 in the original approved Application and signed Data Use Agreement.

### **What information is required in order to submit a data request?**

According to both CO 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 and experience 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 data release applications and advises the APCD Administrator by:

1. Making a recommendation for approval, or
2. Requesting changes to the application or additional information such that a recommendation for approval can be made.

**What kind of organizations can get information from the CO APCD?**

Under CO APCD statute and rule, both public and private entities may receive data or reports subject to review and recommendation for approval by the DRRC. Organizations that have requested information from the CO APCD thus far include university researchers, divisions of Colorado state government, non-profit organizations, health care providers, and private firms developing new pricing models for health care services.

**What can CO 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 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 support marketing activities or to generate financial gain for 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 or used to identify individuals.

**Can an organization charge others for information it gets from the CO APCD?**

Under an approved request, use of the released data is limited to the specific purpose 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 CO 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 CO APCD data and 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 APCD statute and rule.

**Could a company get a report from the CO 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 obtaining direct 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, health care or lower costs. Release of names or other identifiers for specific patients can only occur in the most unusual public health circumstances or under research protocols that require patient authorization or Institutional Review Board approval under HIPAA.

### **What happens if an entity misuses CO 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 HIPAA compliant Data Use Agreement with the CO APCD Administrator and agree to the following:

- Restrictions on data disclosure and prohibitions on re-release of the data.
- Prior approval from the CO APCD Administrator is required prior to public release of any reports based on the data. The CO 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 CO APCD data.
  - b. Result in denial of future access to CO 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 CO APCD Administrator held accountable for the use of CO APCD data?**

Under CO APCD statute, the Administrator is required to provide an annual report to the Governor and General Assembly summarizing various aspect of APCD development and operations.

The CO 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 privacy and security laws and regulations, including HIPAA.
2. The number of requests for data and reports from the CO 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 exception pursuant to which the use or disclosure was approved, and whether a data use agreement was executed for the use or disclosure. To protect CIVHC and CO APCD interests, all recipients of data must sign a data use agreement prior to receipt of data.
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 CO APCD is designed and operated. Not only is data encrypted and protected on secure systems, but personal information will never appear in any public CO APCD data output or report.





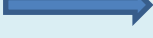
**Data Security:** When carriers submit files to the CO APCD, the datasets are always encrypted and sent over a unique secure connection to the CO APCD data management vendor. This connection is limited to a pre-determined list of users and IP addresses (internet connections) reserved for the carriers submitting the data. The servers holding CO 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 CO APCD (e.g., from an employee’s home computer). Further, the data manager conducts quarterly “penetration” (hacker) testing of the CO 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 CO APCD data output or report. All requests for CO 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 CO 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 below. All information in the CO 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.

Un-encrypted Data	Becomes	Encrypted Data
Name: Jane Doe		3INDzLjr2SnG8ma4wvLoXw==z
DOB: 1/1/1980		5lZB3CeWebVUYm2u9b1+
Gender: F		9D4QK0mn5hE1/2F5
Admit Date: 2/1/2010		bF6R7dA9rdz3k2dez
Discharged: 2/5/2010		s7J51mWcr7WQ4CmN

**Could an employer or a law enforcement agency requisition information about an individual from the APCD?**

Based on the CO APCD statute and HCPF rules, the CO 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 CO 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.

# CO APCD Oversight Roles and Relationships

