Colorado All Payer Claims Database

FAQs - Privacy and Security

CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

Why should the government, or a private entity like CIVHC, be able to collect information about the health care services I'm using?

The CO APCD is designed to identify population patterns. Health care is unique in that there is virtually no publicly available information on cost and quality. The intent of the CO APCD is to even the playing field for consumers, businesses and others to make educated and informed decisions that will improve the health of Coloradans. The aggregate data in the CO APCD will allow consumers and others to answer questions such as:

- What will this procedure cost me?
- Which providers provide the best quality at a reasonable cost?
- How does payment differ by location?
- What are the trends in disease prevalence?
- What are the trends in treatment choices?
- How does quality vary across regions of the state?

How does the CO APCD keep information private and safe?

The safety and privacy of personal information is a foundational principle of how the CO APCD is designed and operated.

Data Security: When carriers submit files to the CO APCD, the datasets are encrypted and sent over a secure connection (File Transfer Protocol or FTP) to the CO APCD Data Manager. The FTP will be limited to a pre-determined list of users and IP addresses (internet connections) reserved for the carriers submitting the data. When the CO APCD Data Manager receives a file, security protocols run automatically, without manual intervention and in a secure environment, to confirm that the files contain the expected information before they are stored in the secured data warehouse.

The CO APCD Data Manager specializes in providing secure solutions that comply with the Health Information Portability and Accountability Act of 1996 (including HITECH act), Federal Information Processing Standards, as well as conforming to standards published by the National Institute of Standards and Technology. The CO APCD Data Manager also engages third party review of its services and uses modern technologies, including advanced encryption, biometrics and intrusion prevention and detection, to secure its facilities providing solutions to healthcare organizations throughout the United States.

Elimination of personal identifiers: As data are loaded into the warehouse, all personal information is removed from the record and replaced with an identification number that is generated by a separate software tool. This tool allows the assignment of an identification number that is completely unique and is not based on reconfiguring personal information.

Additionally, birth date will be replaced with age category and zip codes will be 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.

The CO APCD has established a data release process for specialized reports and data requests. All requests 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 will review the request and advise CIVHC 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.

Will my medical information be at risk to data breaches I've read about?

No. The CO APCD data warehouse is never exposed to the public and is housed in a high security facility, with role-based security. Data is encrypted both in motion and at rest. Furthermore, all personal information is removed from the record and replaced with an identification number that is generated by a separate software tool. This tool allows the assignment of an identification number that is completely unique and is not based on reconfiguring personal information. Additionally, birth date will be replaced with age category and zip codes will be reduced to the first 3 digits (or "000" if from a zip code with fewer than 20,000 people).

How can you guarantee us that no one will hack into the CO APCD?

It's impossible for any organization to make such a guarantee. However, we take our responsibility to safeguard the information in the database very, very seriously—and will do everything in our power to ensure its security. A proven track record of data security was one of our paramount criteria for selecting the database vendor. The CO APCD Data Manager has robust systems in place for protecting the data. They use best practices and follow widely-accepted standards for their security controls. They conduct regular tests in which they hire hackers to try to penetrate their defenses, and adjust their systems as necessary. They require and provide continuing education to their staff about the latest in security and protection.

Moreover, CIVHC holds the CO APCD Data Manager accountable for its security practices through our contract with them, so they are highly motivated to maintain a strong security posture.

In the very unlikely event that someone was able to penetrate the multiple levels of security that the CO APCD Data Manager uses, data in the CO APCD is encrypted such that it would be unintelligible.

CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

As a patient, can I opt out of having my information included in the APCD?

Under Colorado state law, the CO APCD collects claims information from insurance companies and public payer programs, such as Health First (Colorado's Medicaid Program), about health care services received by Colorado residents. Federal laws, including the Health Insurance Portability and Accountability Act (HIPAA), permit such disclosures from payers to be made. Because the CO APCD is designed to facilitate the reporting of aggregated health care and health quality data in a manner that results in transparent and public reporting of safety, quality, efficiency and cost information for all Coloradans, there is not a mechanism for individuals to opt-out. Like other states that support APCDs, CO APCD law requires that all state and federal laws be strictly met in order to protect the database and the sensitive information it holds.

Will the detailed health history and family health questionnaire that I filled out for my doctor or insurance company be stored in the CO APCD?

The CO APCD isn't a medical record, and doesn't capture information from questionnaires or your doctor's notes. It only includes the information from insurance claims, such as what services were received and how much was paid for those.

Insurance claims show diagnosis codes, not just treatment codes, so could someone get into the CO APCD and see that I have cancer, or AIDS?

The CO APCD is built from the same information found on insurance claims, including diagnoses and procedure codes. However, the CO APCD is very different from insurance claims systems, physician billing systems and the millions of Explanation of Benefit letters sent to patient homes. All of those are designed to identify and track specific patients. The CO APCD however, is designed to aggregate data in order to perceive and display patterns of cost and utilization. While identification data are in the CO APCD, they are encrypted and stored separately from the utilization and cost data.

How can you adequately protect the health information of people living in rural areas where the population is so low that it wouldn't be difficult to determine who a person of a certain age with a certain diagnosis is?

Colorado does have a lot of sparsely populated areas. That's why it's so important to understand that the reports from the CO APCD gathers all the information for zip codes with fewer than 20,000 residents into one zip code of "000"—it won't be possible to tell where those claims came from.

CIVHC

CENTER FOR IMPROVING VALUE IN HEALTH CARE

If you take out the zip codes from sparsely-populated areas, won't it be difficult to be able to see health care utilization from, say, the eastern plains?

Five-digit zip codes are retained and encrypted in the database. Some analysis of CO APCD data will allow distinctions among geographic areas. However, any reports that are produced from this data will group zip codes with fewer than 20,000 residents into a single group.

I've heard that 87 percent of the population can be accurately identified with just 3 pieces of information: zip code, birthday and gender, so can't someone get into the CO APCD and get enough information to steal my identity?

The CO APCD does not provide that kind of information in published reports or datasets. Reports distill zip codes down to 3 digits, and strip them out entirely if fewer than 20,000 people live there. Date of birth will be changed to age or age range.

What do you mean by "date of birth will be changed to age or age range"?

Date of birth is in the CO APCD in an encrypted state. Depending on the type of report pulled from the database, it is translated into either an age or age range. Published reports do not reflect dates of birth.

What would a hacker see if he got into the database?

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.

How does the CO APCD Data Manager ensure their employees with access to the database don't hack in remotely or that a disgruntled former employee doesn't hack in?

The CO APCD Data Manager does not allow their employees to have remote access to the database or the infrastructure that supports the Co APCD. When the CO APCD Data Manager terminates an employee or the employee leaves, that individual's "role" relative to the database—i.e., access—is also terminated. This process includes removing physical and electronic access.

CIVHC

CENTER FOR IMPROVING VALUE IN HEALTH CARE

Could an employer or law enforcement agency requisition information about an individual from the CO 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, etc.). Any data that was released under such circumstances would, however, require that HIPAA's privacy standards be met.

Could the federal government request information about an individual from the CO APCD?

It's possible that there could be homeland security or public health needs that would generate such a need. Again, any data released under such a scenario would still have to comply with HIPAA privacy standards.

Will you ever release identified information?

HIPAA allows the release of certain, limited data fields for very narrow purposes: public health activity and research activity. The CO APCD DRRC reviews every request for CO APCD data reports to ensure that no information is released that goes beyond HIPAA rules.

Is CIVHC going to sell my health information to make the CO APCD sustainable?

The CO APCD was created because of the important benefits it can provide to Coloradans, but in this era of tight budgets no dollars were allocated. Instead, the rules for the CO APCD allow data to be released in ways that are consistent with state and federal privacy laws and for the Administrator to be reasonably compensated for costs with operating the CO APCD. Any data reports granted will strictly follow HIPAA privacy and security rules.