Prescriptions and Your Privacy (California Medical Privacy Series) [1]

1. What does this guide cover?

This guide discusses why prescription privacy is important and how prescription information may be used or disclosed. It focuses specifically on prescription privacy in California.

2. Why is prescription privacy important?

Information about your prescriptions, dosages, dates filled, and prescribers can reveal a lot about your medical history – in some cases almost as much as a comprehensive medical record.

3. Who has access to your prescription information?

California and federal laws restrict certain disclosures of health and medication information, including prescription data. However, prescription information is widely circulated in less publicly known ways. These include:

- to pharmacy benefit managers;
- in prescription drug reports;
- by prescription data miners; and
- through prescription drug monitoring programs.

For more information about how medical information may generally be used and disclosed, see PRC’s guide, How is Your Medical Information Used and Disclosed? (California Medical Privacy Series) [2].

a. Pharmacy benefit managers

What is a pharmacy benefit manager?

Pharmacy benefit managers (PBM) administer drug benefit programs for health plans. Large public PBMs include Express Scripts (a standalone PBM), CVS Health (a combined national pharmacy chain and PBM), and United Health/OptumRx/Catamaran (an insurer-owned PBM). The largest private PBM is Prime Therapeutics, which is owned by a group of state Blue Cross/Blue Shield plans.

What do pharmacy benefit managers do?

PBMs manage all aspects of prescription drug plans - they:
- **set up pharmacy benefits**
  PBMs establish formularies (lists of covered drugs) and payment and co-payment structures on behalf of prescription drug plans.

- **process prescription claims**
  When you go to a pharmacy, the pharmacist electronically submits your prescription to the PBM your plan contracts with to see if your plan covers the drug, how much it pays, and what your co-payment is. PBMs charge the plans a fee for processing prescription claims.

- **provide cross-pharmacy data for drug interactions**
  This PBM function can benefit people who fill prescriptions at more than one pharmacy. For instance, you may get a drug at one pharmacy that is incompatible with a prescription obtained at a different pharmacy. This function enables your pharmacist to know about your other prescriptions and advise you based on this knowledge.

- **operate mail order pharmacies**
  PBMs are in the mail-order drug business and are paid directly by drug plans when they fill mail order prescriptions.

For more general information about PBMs, see [PBM Fiduciary Duty and Transparency](http://www.prescriptionpolicychoices.org) by Prescription Policy Choices (a nonprofit, nonpartisan organization providing research and information on prescription drug policy).

**How do PBMs affect your prescription privacy?**

PBMs have access to a lot of sensitive information. As the manager of prescription claims and benefits, a PBM has all of your prescription information: the medication, dosage, number of refills, who prescribed it, and on what date. It also has your name, date of birth, address, phone number, credit card number, and prescription plan sponsor and account number.

PBMs are subject to both federal and California medical privacy laws as business associates (under HIPAA) or contractors (under California’s Confidentiality of Medical Information Act). For more information about CMIA and HIPAA, see [PRC’s health and medical privacy guides](http://www.prescriptiondrugsafety.org).

**Noncompliance and poor business practices**

Despite their legal obligations, the privacy and security practices of one PBM in particular have been problematic.

In 2009, the Federal Trade Commission (FTC) fined CVS Health, a national pharmacy chain and a PBM $2.25 million for HIPAA and FTC violations, for throwing pill bottles into open dumpsters with patient names, addresses, prescribing physicians’ names, medication and dosages, along with medication instruction sheets with personal information, computer orders that included consumers’ personal information, and credit card and insurance card information, including, in some cases, account numbers and driver’s license numbers. As a result, CVS was actively monitored by the U.S. Department of Health and Human Services until 2012 and will continue to be monitored by the FTC until 2030.

In 2009, six Texas community pharmacies brought a lawsuit against CVS Caremark. In [The Muecke Company, Inc. v. CVS Caremark Corporation](http://www.prescriptionpolicychoices.org) plaintiffs alleged that CVS Caremark used prescription and personal information it gathered from non-CVS pharmacies as a PBM and mined this data to identify individual patients’ buying practices, physicians’ prescribing practices, and individual pharmacy business volume. It further alleged that CVS Caremark contacted consumers by mail and telephone to urge them to use CVS retail or mail order stores, and targeted physicians in an attempt to change their prescribing practices to include drugs from CVS Caremark-favored drug makers. Ultimately this case was resolved through arbitration, but it highlights significant privacy concerns with the PBM business model.

**Prescription data sales**

PBMs routinely sell de-identified or aggregated data (data from which personally identifiable information has been removed) to data miners. Data miners resell the data in reports. These sales are legal because de-identified data is not covered by California or HIPAA privacy and security requirements. To learn more about this, see [Prescription data mining](http://www.prescriptionpolicychoices.org) below.

**Insurance reporting**

PBMs don’t sell individual prescription drug reports directly to insurers. Instead, they sell identifiable prescription data to companies that compile the reports. For more information, see [Prescription drug reports](http://www.prescriptionpolicychoices.org) below.

**What rights do you have regarding your prescription information and PBMs?**

As business associates/contractors of health plans, PBMs must comply with HIPAA and California’s Confidentiality of Medical

In particular, you may want to access your records to make sure they are accurate and consider requesting an accounting of disclosures from a PBM. Contact your insurer to find out which PBM your plan contracts with.

Since the Affordable Care Act became law in March 2010, health insurers can no longer deny coverage based on any pre-existing condition and they may not require your medical records as part of the application. If you’re applying for life or long term care, disability, or certain types of automobile insurance, you may be asked to authorize the release of your medical records. Certain insurers (but NOT health insurers) can use that information to underwrite your policy. Incorrect information could affect your insurability or your premium. It is in your interest to know if those records are correct and complete.

b. Prescription drug reports

What is a prescription drug report?

Two companies, Milliman and OptumInsight (formerly Ingenix), compile individual prescription information into prescription drug reports. A report covers your prescriptions for up to five years, including dosages, dates, refills, and prescribing doctors. The reports also provide a risk score based on the drugs you take. Higher scores indicate potentially higher medical costs.

How are prescription drug reports used?

Insurers buy prescription drug reports to verify the information in your application for individual life, long term care, or similar coverage. Insurers also use the reports to determine risk, set premiums, and decide whether to insure you. They can obtain this information because you are typically required to sign an authorization when you apply for individual insurance policies where your health is a risk factor (though NOT health insurance).

What rights do you have regarding your prescription drug report?

You may access your prescription report and dispute inaccuracies, in addition to other rights provided by the Fair Credit Reporting Act (FCRA) [7]. There will be a prescription report on you only if you have applied for life, long-term care, or similar insurance in the last five years. To find out if a report exists, obtain a copy, and request corrections, contact Milliman and OptumInsight [8]. See PRC’s resources on Credit Reports [9] for more information about your rights under the FCRA.

Prescription reporting companies are consumer reporting agencies (CRAs) subject to the FCRA because they compile and analyze consumer information (prescriptions) and furnish it to insurers to use in determining individuals’ eligibility for insurance. See this Federal Trade Commission (FTC) consent order [10] for more information.

c. Prescription data miners

What is prescription data mining?

Prescription data miners use de-identified or aggregated prescription data to generate reports about doctors’ prescribing practices. Pharmaceutical companies buy the reports to strategically market drugs to doctors based on information about the doctor’s prescribing history (called detailing).

Data miners buy prescription information from pharmacies and pharmacy benefit managers (PBMs). The data comes to them encrypted by applications that the data miners themselves install at the data source. They then remove the elements that identify individuals. However, individual data is still identified by a number and can be tracked over time to show other prescriptions filled for that number, how long the person takes a drug, and if a drug is discontinued or a new one prescribed.

The data miners’ de-identification process is sufficient to remove the data from the protection of California’s Confidentiality of Medical Information Act and HIPAA. Data miners keep the prescriber’s name, the name of the drug, and the dosage, which are the basis of the reports they sell.

Data mining is a big business. As an IMS statistician wrote in an internal company report, Data Mining at IMS America How We Turned a Mountain of Data into a Few Information-rich Molehills [11]: “Research has shown that winning just one more prescription per week from each prescriber, yields an annual gain of $52 million in sales. So, if you’re not targeting with the utmost precision, you could be throwing away a fortune.”

And, to quote a judge in a case that tested a New Hampshire law to restrict prescription data mining similar to Vermont’s: “[t]he fact that the pharmaceutical industry spends over $4 billion annually on detailing bears loud witness to its efficacy.” (IMS Health Inc. v. Ayotte, 550 F.3d 42, 56 (1st Cir. 2008), cert. denied, 129 S. Ct. 2864 (2009))
How does prescription data mining affect your privacy?

Data mining exposes vast amounts of prescription information to an unregulated and largely nontransparent industry. Data miners themselves are in charge of handling prescription data securely, de-identifying the data, and refraining from re-identifying the data. This raises significant privacy questions and concerns, but unfortunately there is little you can do to address them.

In addition, prescription data mining can intrude on the presumed privacy of the doctor-patient relationship. Pharmaceutical companies buy data miners’ reports with the intent to influence doctors’ prescribing habits. They are assisted in this by the American Medical Association, which sells the names of its member physicians. This allows the pharmaceutical companies that buy the reports to connect patient-de-identified prescription information with the doctor who prescribed the medication, and for company sales representatives to target those doctors with specific information about their prescribing practices.

**Prescription data mining is not going away any time soon.** In 2011, the U.S. Supreme Court invalidated a Vermont law regulating prescription data mining by permitting it for research purposes, but not for marketing to doctors. See *Sorrell v. IMS Health, 131 S.Ct. 2653 (2011)* [12] and the SCOTUSblog [13].

Do you have any rights regarding the use of your prescription information by data miners?

Not really. Your only real option is to ask your physician if he or she is in the [AMA’s Physician Data Restriction Program (PDRP) [14], which allows doctors to opt out of having their prescribing information used for pharmaceutical marketing. Even if a doctor opts out, the AMA can still sell personal and practice information from its Physician Masterfile. Pharmaceutical companies that buy Masterfile profiles to match with data miners’ reports on doctors’ prescribing practices have to agree not to provide an opted-out doctor’s prescribing data directly to their salespeople. However, a company may still use the information for targeted marketing. And in any case, the prescribing doctor’s name is already in the information the data miner extracts from your prescription record.

d. Prescription drug monitoring programs

**What is a prescription drug monitoring program?**

A Prescription Drug Monitoring Program (PDMP) is a state-run electronic database that collects information about and tracks controlled substance prescriptions.

**California’s PDMP: CURES**

California’s PDMP, called CURES (Controlled Substance Utilization Review and Evaluation System) [15] is administered by the Attorney General’s office, by its Department of Criminal Justice Information Services. Started in 1939, CURES is the oldest such program in the U.S. States.

California physicians (including veterinarians) and pharmacists who dispense Schedule II–IV controlled substances [16] (opiates, anti-depressants, narcotics, anabolic steroids, hallucinogens, and stimulants) must report all prescriptions for these drugs weekly to the Attorney General’s office, on a form called the Prescribers’ Direct Dispensing Log [17]. See Cal. Health & Safety Code § 11190 [18]; Cal. Bus. & Prof. Code § 4170 [19].

Each report contains the following:

- prescriber’s name, address, telephone number, license type and number, and federal controlled substance registration (DEA number);
- pharmacies additionally include the pharmacy prescription number, license number, and federal controlled substance registration number;
- patient’s full name, address, date of birth, gender, prescription number, and diagnosis code;
- drug name, National Drug Code number, quantity and strength of prescription, and the date it was dispensed.

The data is available to state, local, and federal agencies for disciplinary, civil, and criminal actions. Upon approval by the Attorney General, other public and private entities may also access de-identified CURES data for educational, peer review, statistical, or research purposes. No data that is disclosed may be further disclosed, sold, or transferred to any third party. Cal. Health & Safety Code § 11165(c) [20]

In addition, health care providers who prescribe or dispense Schedule II–IV drugs may apply to access CURES data online to
learn about their patients’ controlled substance prescription history. One purpose of this is to help identify patients who are being over-prescribed certain drugs.

How does the CURES database affect your privacy?

CURES affects your privacy by putting personally identifiable medical information into yet another database that many individuals and agencies may access.

Do you have any rights with regard to prescription information in the CURES database?

Individuals have no right to access their own CURES records. The CURES database is only accessible to health care providers and pharmacists who register with the California Department of Justice, and law enforcement and regulatory boards authorized by statute. Cal. Health & Safety Code § 11165(c) [20]

The California Attorney General’s office considers requests for release of controlled substance history, but rarely grants them. De-identified CURES data has been used for research.

This lack of transparency, along with the U.S. Department of Justice’s goal of linking all state prescription drug monitoring programs, highlights a need for federal standards for the privacy and security of PDMP data and effective penalties for violations.

4. Additional Resources

You can find legislative information, including current California law on the California Legislation Information website [21].

California Attorney General’s Office:

Privacy-related bills [22]

Your Patient Privacy Rights: A Consumer Guide to Health Information Privacy in California; Tips for Consumers [23]

U.S. Department of Health and Human Services (HHS):

Information about accessing and correcting medical records [24].

Information about your rights under the HIPAA Privacy Rule [25].

The HHS Office of Civil Rights [26] has additional health privacy information for consumers.

American Medical Association’s Prescription Data Restriction Program [27]

California’s Prescription Drug Monitoring Program - CURES:

Learn more about California’s Prescription Drug Monitoring Program, CURES [28].

To find out if you take a prescription that must be reported to the CURES database, see Cal. Health & Safety Code, §§ 11055-11057 [29].

Originally funded in 2012 with cy pres award from Rodriguez et al. v. NDHealth et al.

Updated in 2017 with funding from the Rose Foundation for Communities and the Environment.


Links