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

1. Introduction

Information about the medications you take is just as personal as your detailed medical history. This is one reason why the laws that protect medical information also protect prescriptions. A list containing your prescriptions, the dosages, the dates filled, and who prescribed them, reveals your medical history almost as effectively as a complete medical record. For obvious reasons, most individuals want to keep prescription information as private as possible, and share it only with their doctors and pharmacists.

Despite many individuals’ desire to restrict how and with whom it is shared, prescription information is used and disclosed in many ways. Sometimes your information is shared with your knowledge and consent, but sometimes it is not. California and federal laws restrict certain disclosures of prescription data.

However, health care providers, health plans, and their business associates or contractors, can use your information without your consent for purposes involving medical treatment or payment of medical bills. Your information can also be used for “health care operations,” generally all administrative functions associated with providing health care. Prescription information may also be available to public health and law enforcement agencies (see Section 5, What Are Prescription Drug Monitoring Programs (PDMPs) and How Can They Affect Your Privacy?).

Under California law, certain sensitive medical information receives special protections. HIV status, psychotherapy notes, and substance abuse treatment information require your signed and dated authorization before they can be disclosed (an authorization you sign should state specifically to whom the information may be released). However, prescription data that can reveal the same sensitive conditions or information about you do not require your authorization to be disclosed. This is an acknowledged gap in the law that remains in search of a solution.

In addition to the routine permitted disclosures (for medical treatment, payment, and healthcare operations), the public is generally unaware that prescription information is widely circulated in other obscure ways, these include:

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

This fact sheet covers these topics.

2. Pharmacy benefit managers (PBMs): what are they and how do they affect your prescription privacy?

a. What is a PBM?

A pharmacy benefit manager (PBM) is a company that administers drug benefit programs for health plans. These include employer-funded plans, managed care organizations, corporations, and unions, as well as Medicaid, Medicare and other federal, state, and local programs (e.g., MediCal and CalPERS). PBMs are called “contractors” under California law and “business associates” under federal rules. A business associate is a third party, bound by a contract, that performs a service on behalf of a health care provider or institution during which individually identifiable health information is created, used, or disclosed.

Contractors and business associates are subject to privacy and data security laws because their functions require access to patients’ personal information just like the health plans they serve. They are covered by California’s Confidentiality of Medical Information Act (CMA) (Cal. Civ. Code §§56–56.37) and are also subject to federal Health Insurance Portability and Accountability Act (HIPAA) regulations. They also operate under agreements that require them to follow California and federal laws that protect the security of medical information.

The U.S. Department of Health and Human Services (HHS) has an online publication concerning business associates and HIPAA [2].

PBMs have existed since the 1980s. They were created to apply managed care’s “rationing” principles to the prescription portion of health plans. PBMs’ roles have expanded over time, and they now manage all aspects of prescription drug benefit plans. PBMs carry out the following functions:

- Set up pharmacy benefits. PBMs establish formularies and payment and co-payment structures on behalf of prescription drug plans. Formularies are lists of drugs that are covered under a plan.
- 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-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 conflicts 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.

As of March 2012, the two largest PBMs—CVS Caremark and Express Scripts/Medco—process the prescriptions of an estimated 200 million people in the U.S. The annual revenues of each of these companies exceed $15 billion.

PBMs are supposed to support the managed care theory of reducing healthcare costs. However, PBMs do not operate in a transparent manner, making it difficult to determine if they actually reduce costs. PBMs negotiate with pharmacies over the amounts they receive for filling prescriptions and negotiate separately with drug plans for what they pay the PBM. This means that a PBM may be paid more by a drug plan than it pays to the pharmacy that fills your prescription. PBMs also benefit financially from buying drugs at a discount from pharmaceutical companies and selling them for a higher price to pharmacies.

Pharmaceutical companies pay PBMs rebates to ensure that their drugs are on a PBM’s formulary list. To help keep costs down, PBMs are supposed to share rebates with the prescription plans that pay for the drugs. However, there is no requirement that PBMs account for how much of the rebate money they keep.

In 2004, then-New York Attorney General Elliot Spitzer sued the PBM Express Scripts for defrauding the state of tens of millions of dollars in rebates and other unethical business practices. The company settled the lawsuit, paying $9.3 million to 29 states to resolve claims of deceptive business practices and up to $200,000 in reimbursement to patients.

The Health Care Reform Act of 2010 requires greater financial disclosure from PBMs on the discounts and rebates they get from pharmaceutical companies and what they pass through to prescription drug plans as cost savings. The intent is to help reduce the cost of prescription drugs and thus of health care overall.

For more information about PBMs, how they operate, and what they mean to you as a consumer, see “PBM Fiduciary Duty and Transparency [3],” by Prescription Policy Choices, a nonprofit, nonpartisan organization providing research and information on prescription drug policy.
Prescription data mining is the business of using de-identified prescription data to generate reports about doctors' prescribing practices, and it is a big business. In 2010, companies engaged in the business

There will be a prescription report on you only if you have applied for

Also see, FCRA, see PRC's notifying individuals who are denied insurance because of their prescription reports and providing them with a means to request a copy of the report and have any errors corrected. For more information on the

Prescription reporting companies are CRAs because they compile and analyze consumer information (prescriptions) and furnish it to insurers to use in determining individuals' eligibility for insurance.

However, in 2007, the Federal Trade Commission (FTC) issued a consent

and federal laws regulating the privacy and security of medical information.

For many years, individuals had no protections with respect to the use of their prescription information in these reports. This is primarily because prescription reporting companies don't fall under the California

A prescription report provides a risk score based on the drugs you take. Higher scores imply potentially higher medical costs. Insurers use electronic prescription reporting services because they are more

b. How do PBMs affect your prescription privacy?

When you fill a prescription you should receive a notice of privacy practices, required by HIPAA, which says the pharmacy may use or disclose your protected health information (PHI) for treatment, payment, or health care operations, and that your consent is not required. The notice of privacy practices will also say that the pharmacy may release your PHI to a PBM to check your eligibility and get approval for your medication. This is how your prescription information is legally disclosed to a PBM.

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. In sum, PBMs have access to a lot of very valuable and sensitive personal information.

Despite its legal obligations, the privacy and security practices of one PBM in particular have been problematic. CVS Caremark is both a national pharmacy chain and a PBM. In 2009, the Federal Trade Commission (FTC) fined the company $2.25 million 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.

Currently, there are at least two lawsuits pending against CVS Caremark alleging illegal use of protected health information.

In The Muecke Company, Inc. v. CVS Caremark Corporation [4], six Texas community pharmacies claim that, instead of maintaining a firewall between their pharmacy and PBM data, as the FTC required when CVS and Caremark merged in 2007, the information is shared. The lawsuit alleges that CVS Caremark uses prescription and personal information it gathers from non-CVS pharmacies as a PBM, and mines this data to identify individual patients' buying practices, physicians' prescribing practices, and individual pharmacy business volume. CVS Caremark then contacts consumers by mail and telephone to urge them to use CVS Caremark retail or mail order stores. CVS Caremark also targets physicians in an attempt to change their prescribing practices to include drugs from CVS Caremark-favored drug makers.

In early 2012, a class action lawsuit filed by the Philadelphia Federation of Teachers Health and Welfare Fund against CVS Caremark was dismissed [5]. The suit alleged that drug manufacturers Eli Lilly, Merck, AstraZeneca, Bayer, and others paid CVS Caremark to use individual consumers' protected health information to send letters to their doctors promoting the manufacturers’ drugs. A federal judge held that the plaintiffs had no actionable claim under Pennsylvania's Unfair Trade Practices and Consumer Protection Law.

In November 2008, Change to Win [6], a group of unions representing about six million workers, accused CVS Caremark’s PBM business of sending letters to doctors to add the Merck diabetes drug Januvia (which costs between five and eleven times as much as other diabetes drugs) to specific patients’ treatments. Merck allegedly paid CVS to send the letters. In addition, Change to Win claims that CVS identified the diabetes patients through a review of prescription claims processed by its PBM unit Caremark.

Despite the dismissal of the Philadelphia Federation of Teachers' lawsuit, there are good reasons for concern that CVS Caremark may use protected information that it collects both as a pharmacy and a PBM for direct marketing purposes. This would violate the company's legal responsibilities under both federal law (HIPAA) and California law (CMIA) to protect the privacy and confidentiality of medical information.

In addition, this would violate protections against selling the data or using it for marketing purposes without patient authorization. (Cal. Civ. Code §§ 1798.91, 56.10(d); HITECH Act § 13406)

c. Selling prescription data.

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 packaged as different types of reports. These sales are legal because de-identified data is not covered by California or HIPAA privacy and security requirements. For more information, see Section 4. What & Prescription Data Mining and How Does It Affect Your Prescription Privacy?

d. Reporting to insurers.

PBMs don't sell individual prescription drug reports directly to insurers. Instead, they sell identifiable prescription data to companies that do. For more information, see Section 3. What Are Prescription Drug Reports and How Do They Affect Your Privacy?

P. What is prescription data mining and how does it affect your prescription privacy?

b. How are prescription reports used?

Insurers buy prescription drug reports to verify what you put on your application for individual, health, or similar coverage. Insurers also use the reports to determine risk, set premiums, and decide whether to insure you. They can obtain this legally protected personal health information because when you apply for most individual policies where your health is a risk factor, you sign an authorization to release it. A prescription report provides a risk score based on the drugs you take. Higher scores imply potentially higher medical costs. Insurers use electronic prescription reporting services because they are more efficient, less time-consuming, and cheaper than requesting your prescription information from each of your health care providers.

c. What rights do you have regarding your prescription drug report?

For many years, individuals had no protections with respect to the use of their prescription information in these reports. This is primarily because prescription reporting companies don’t fall under the California and federal laws regulating the privacy and security of medical information.

However, in 2007, the Federal Trade Commission (FTC) issued a consent [9] declaring Ingenix and Milliman to be consumer reporting agencies (CRAs) subject to the Fair Credit Reporting Act (FCRA). Prescription reporting companies are CRAs because they compile and analyze consumer information (prescriptions) and furnish it to insurers to use in determining individuals' eligibility for insurance. The FTC’s action settled claims that the companies violated the consumer-reporting law by failing to notify insurers of their responsibilities under the FCRA. These responsibilities include, among other things, notifying individuals who are denied insurance because of their prescription reports and providing them with a means to request a copy of the report and have any errors corrected. For more information on the FCRA, see PRC’s Fact Sheets on Credit & Credit Reports [10].

Also see, PRC Fact Sheet 8: Medical Records Privacy, Section 40 [11], for more on CRAs that report on prescription drugs for insurance purposes.

The FTC’s determination gives individuals some recourse, but it does nothing to protect the privacy of their medical information. Individuals would have greater privacy and security protections if prescription reporting companies were considered covered entities under HIPAA because they access or receive protected health information. However, this is unlikely to happen any time soon.

There will be a prescription report on you only if you have applied for individual, health, 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, call Milliman 1-822-877-211-4816 and Ingenix [13] at 888-206-0335.

4. What is prescription data mining and how does it affect your prescription privacy?

a. What is prescription data mining?

Prescription data mining is the business of using de-identified prescription data to generate reports about doctors' prescribing practices, and it is a big business. In 2010, companies engaged in the business
together generated $9 billion total income by selling thousands of market research reports each costing thousands of dollars.

Pharmaceutical companies buy the reports to use for a practice known as “detailing.” Detailing involves strategically marketing drugs to doctors based on a sales representative’s knowledge of which drugs doctors prescribe for which conditions.

Data miners buy prescription information from pharmacies and 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, although the 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 the CMA and HIPAA. In other words, an expert’s determination that the risk of individual identification is “very small” is sufficient. Data miners keep the prescriber’s name, the name of the drug, and the dosage, which are the basis of the reports they sell.

No current state or federal law applies in this context to re-identifying data that has been de-identified. Prescription data miners have the ability to re-identify individual data based on the number assigned to it, and they operate separately from the entities—health care providers, health plans, health care clearhouses, and their contractors or business associates—that do have legal obligations.

b. How does prescription data mining affect your privacy?

Although prescription data miners do not identify you as an individual who takes a certain medication, the practice of prescription data mining still affects your privacy. To begin, it exposes vast amounts of prescription information to an unregulated industry unrelated to medical treatment, bill payment, or even health care operations. Data miners themselves are in charge of handling prescription data securely and de-identifying it.

Data miners have the ability to re-identify prescription information, but do they? And if they do re-identify data, what are they doing with it? Unfortunately there are no clear answers, and data miners and any re-identified data exist outside laws that protect the privacy of medical information.

Finally, prescription mining intrudes on the presumed privacy of the doctor-patient relationship. Pharmaceutical companies buy data miners’ reports with the intent to influence doctors’ prescribing habits. So, in effect, a third party whose presence you never consent to—a pharmaceutical sales representative—is in the room with you and your doctor.

A pharmaceutical sales rep’s job is to increase her company’s profits by persuading your doctor to prescribe her company’s drug. This drug may not be right for your condition, may be more expensive than an effective drug you already take, or may have riskier side effects. Although your doctor may appreciate the information (and samples) that sales representatives provide, she can get timely, accurate, and disinterested information about current and new drugs from other sources, for example, a subscription to the bi-weekly, independent Medical Letter on Drugs and Therapeutics.[14]

c. Prescription data mining is not going away any time soon.

The Supreme Court recently invalidated a Vermont law that attempted to regulate prescription data mining by permitting it for research purposes, but not for marketing to doctors. The Court agreed with the data miners’ argument that the law was an unconstitutional regulation of commercial speech and a violation of their corporate First Amendment rights. (Sorrell v. IMS Health, 131 S.Ct. 2653 (2011) [15]) For more information on the Sorrell case see the Electronic Privacy Information Center’s (EPIC) website.[16]

Data miners say their reports serve a public interest because they can be used for research purposes and to track drug safety problems. An example of this is the use of de-identified prescription data to study the utilization and effects of drugs in large populations in order to measure the probability of beneficial and adverse effects, or tracking the increase or decrease in the utilization of specific drugs.

However, this is not what drives the business of prescription data mining. As an IMS statistician wrote in an internal company report, titled “Data Mining at IMS America How We Turned a Mountain of Data into a Few Information-rich Molhehils[17]”: “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))

One way to end this questionable use of prescription information would be to add physicians’ names to California’s and HIPAA’s list of what constitutes protected health information, which would put it off limits to data miners.

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

Consumers really do not have any rights or remedies when it comes to prescription data mining. Because the information in the reports is de-identified, they are not considered to be consumer reports under the Fair Credit Reporting Act. Unfortunately, there is no current California or federal law that keeps your prescription data out of the hands of the data miners. Data miners had a bill pending in 2010 that would have prevented the sale of doctors’ prescribing data for marketing purposes (AB 2112, Monning [18]). However, even if the bill had passed, the Supreme Court’s Sorrell v. IMS decision would have nullified it.

Your only real option is to ask your physician if she is in the AMA’s Physician Data Restriction Program (PDRP) [19], which allows doctors to opt out of having their prescribing information used for pharmaceutical marketing. Even if a doctor opts out, the AMA continues selling her 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 option-out doctor’s prescribing data directly to their salespeople. However, a company may still use the information for targeted marketing.

The Physician Masterfile was started in 1906 to protect the public against fraud by providing a list of who is licensed to practice medicine. State medical boards still use the Physician Masterfile to prevent fraud and verify the credentials of doctors coming from another state. The Masterfile contains the name, practice location, specialty, education and training, licenses, and disciplinary history for nearly every doctor in the U.S., including the two thirds who are not AMA members, totaling almost a million individuals.

A conflict between the Masterfile and the PDRP arises from the fact that the AMA made approximately $45 million from sales of Masterfile data in 2007 (the last year for which a revenue figure is available). The AMA has little incentive to promote an option for doctors to prevent information about their prescribing habits from being used by drug marketers because it sells Physician Masterfile data to pharmaceutical companies. These companies then combine them with prescription data mining reports to build profiles for their salespeople to use to persuade doctors to prescribe a company’s drugs.

5. What are prescription drug monitoring programs (PDMPs) and how can they affect your privacy?

a. What is a prescription drug monitoring program?

A Prescription Drug Monitoring Program (PDMP) is a statewide, government-administered electronic database that collects specific information about prescriptions filled for certain types of pharmaceutical drugs. As of March 2012, PDMPs operate in 37 states, and 11 more have passed legislation to create them. Only two states, Ohio and Kentucky, currently share prescription drug information. The U.S. Department of Justice has developed a software platform—PMX [20]—to facilitate sharing among all state PDMPs. It is also providing funding to help states implement sharing prescription data through PMX.

California’s PDMP, called CURES (Controlled Substance Utilization Review and Evaluation System), 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 consider PDMPs a tool for addressing the problems of prescription drug abuse, addiction, and diversion of pharmaceutical drugs into illegal markets.

b. How does CURES work?

California physicians (also veterinarians) and pharmacists who dispense Schedule II–IV controlled substances (in general, 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 [21]. (Cal. Health & Safety Code § 11190; Cal. Bus. & Prof. Code § 4170) 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.

All of this information makes up the CURES database. 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))

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. (Cal. Health &
The U.S. Department of Health and Human Services has information about accessing and correcting medical records. HHS also provides information about HIPAA.

boards.page http://www.mbc.ca.gov/consumer/access_records.html

The Medical Board of California's "Patient Access to Medical Records." The website also has a complaint form if a health care provider or health plan has not complied with your request.

State medical boards:

You can find legislative information, including current California law on the California Legislation Information website:


U.S. Department of Health and Human Services:

The U.S. Department of Health and Human Services has information about accessing and correcting medical records. HHS also provides information about HIPAA.

U.S. Department of Health and Human Services
Office of Civil Rights

Safety Code § 11165.1(a)(1)): One purpose of this is to help identify patients who are being over-prescribed certain drugs.

Currently, CURES reporting is required only for controlled substances on the Schedule II-IV drug lists. However, there are ongoing legislative efforts to require a prescription for over-the-counter cold and allergy remedies that contain pseudoephedrine.

**c. How does the CURES/PDMP database affect your privacy?**

CURES affects your privacy by protecting personally identifiable medical information into yet another database to which many individuals and agencies have access, even if access is not entirely unmediated. Although the law doesn’t label prescriptions for controlled substances as "sensitive" information or give it special protection, many individuals believe it is extremely sensitive as far as their privacy is concerned. Eventual interstate links mean that prescription data will be widely shared to prevent doctor-shopping, drug abuse, and illegal diversion.

**d. What rights do you have with regard to prescription information in the CURES database?**

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. (H&S § 11165(c)) Individuals have no right to access their own CURES records. Requests for release of controlled substance history, including subpoenas, are considered by the Attorney General’s office, but are rarely granted. 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 strict federal standards for the privacy and security of PDMP data and effective penalties for violations. State laws vary greatly, with California’s being generally more protective than most. Federal standards should include:

- **Notice.** When you fill a prescription for a drug that will be reported to a PDMP, you should be specifically notified of that;
- **Access.** You should have the right to access and correct your PDMP record;
- **Accounting of disclosures:** You should have the right to know who has accessed your PDMP record;
- **Best security practices.** Security should meet the highest industry standards for maintaining data, including access controls and real-time audits of access, and for transmitting data;
- **Subpoena required** for law enforcement access;
- **Only de-identified data** for statistical, research, or educational uses;
- **Stringent civil and criminal penalties** for improper use or disclosure of PDMP data;
- **Private right of action** for data breaches and improper disclosures.

6. Conclusion

Prescription information is legally used and circulated in many ways that do not require your consent. Some, like California’s CURES program, do not even require notice when your prescriptions for controlled substances are sent to a state database. Widespread electronic distribution of prescription data is concerning, not least of all because of the well-publicized insecurity of digital information, whether from hacker attacks, loss or theft of computers and storage devices, or insider abuses. The absence of laws prohibiting re-identification of medical information, especially by data miners and others operating outside the boundaries of the CMIA and HIPAA, is a serious omission.

7. Tips for safeguarding your prescription information

After reading this Fact Sheet on prescription information and privacy, you know that you have only limited control over the flow of this data. Still, the more you know, the better able you are to maximize your limited privacy rights.

1. Educate yourself. Ask questions about your health care providers’ privacy practices—including those of your pharmacist and the PBM that manages your prescription plan. Read their privacy notices and ask questions about what you don’t understand.

2. Talk to your provider about your privacy concerns. Ask providers who prescribe drugs for you if they’ve opted out of sharing their prescription data with pharmaceutical companies via the AMA’s Prescription Data Restriction Program.

3. Assert your consumer rights under the Fair Credit Reporting Act. Find out if you have a prescription drug report with Milliman or Ingenix. If you do and you believe it contains incorrect information, ask to have it corrected.

4. Pay your medical and prescription bills on time. Unpaid bills may go to a collection agency or end up as a negative entry on your credit report. As you know from receiving Explanations of Benefits (EOBs), statements that are not bills, and statements that are bills, the process of sorting out and paying what you owe for medical care can be confusing. Keep current with your medical bills and dispute what you believe are errors in writing both the health provider and insurance company. Try to resolve disputes before bills are referred to a collection agency and/or the credit bureaus.

5. Where there’s a right to obtain a copy of your prescription record and an accounting of disclosures, take advantage of it. You can request your prescription record now from health care providers, health plans, pharmacies, PBMs, and prescription reporting companies. When recent changes to the HIPAA regulations become final you will also be able to request an accounting of the disclosures of your prescription information. Check the information for accuracy and request to have incorrect information corrected or amended. Keep in mind that the entity that has the information has the final word on changes and amendments to its records. See this sample letter [22] for requesting a copy of your medical records.

6. Keep your own record of your prescriptions as a reference. This is essential to being able to correct any errors you find in your prescription records that are maintained by others.

7. Complain. If you think your rights have been violated or your concerns have been ignored, make a written complaint to your provider or health plan. If the problem is not resolved, you may complain to the U.S. Department of Health and Human Service’s Office of Civil Rights [23]. If you feel that a pharmacist has failed to maintain the confidentiality of your prescription information or has entered it incorrectly on the label, the California Board of Pharmacy has a complaint form [24]. It also posts a patient Bill of Rights [25] that includes a right to confidentiality of your pharmaceutical information.

8. Contact your representatives in Congress and in your state legislature if you feel stronger laws to protect your medical privacy are needed. Think of complaining to a representative or the Office of Civil Rights as a long-term process, rather than an immediate solution to what you see as a problem. If enough complaints accumulate, it can alert lawmakers to deficiencies in health privacy laws.

8. Resources

PRC Fact Sheets:

Fact Sheet 8: Medical Records Privacy http://www.privacyrights.org/fs/fs8-med.htm [26]

Fact Sheet 8a: HIPAA Basics: Medical Privacy in the Electronic Age http://www.privacyrights.org/fs/fs8a-hipaa.htm [27]

California Law:

You can find legislative information, including current California law on the California Legislation Information website: http://leginfo.legislature.ca.gov/ [28].

State medical boards:

The Medical Board of California’s “Patient Access to Medical Records.” The website also has a complaint form if a health care provider or health plan has not complied with your request. http://www.mbc.ca.gov/consumer/access_records.html [7]

To link to medical boards in other states, visit the American Medical Association website: http://www.ama-assn.org/ama/pub/education-careers/becoming-physician/medical-licensure/state-medical-boards.page [29]

U.S. Department of Health and Human Services:

The U.S. Department of Health and Human Services has information about accessing and correcting medical records. HHS also provides information about HIPAA.

U.S. Department of Health and Human Services
Office of Civil Rights

4
Prescription Reporting Companies:

To obtain your record from a prescription reporting company contact Ingenix (MedPoint report) at 888-206-0335 and Milliman (IntelliScript report): [webpage](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/medicalrecords.html) [12], 877-211-4816.

AMA Prescription Data Restriction Program:

If your health care provider is not aware that she can opt out of having her prescribing information used by pharmaceutical company sales representatives, refer her to the AMA’s Prescription Data Restriction Program. She can opt out whether or not she is an AMA member. [AMA Prescription Data Restriction Program](http://www.ama-assn.org/ama/pub/about-ama/physician-data-resources/ama-database-licensing/amas-physician-data-restriction-program.page) [19]

California’s Prescription Drug Monitoring Program: CURES:

Learn more about California’s Prescription Drug Monitoring Program, CURES, [webpage](http://oag.ca.gov/cures-pdmp) [30]

To find out if you take a prescription that must be reported to the CURES database, see Health & Safety Code, §§ 11055-11057. [webpage](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=11001-12000&file=11053-11058) [31]

---

Source URL (modified on September 27, 2016): [webpage](https://www.privacyrights.org/consumer-guides/your-prescriptions-and-your-privacy-california-medical-privacy-series)

Links
[1] [webpage](https://www.privacyrights.org/consumer-guides/your-prescriptions-and-your-privacy-california-medical-privacy-series)
[2] [webpage](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html)
[3] [webpage](http://www.policychoice.org/pharmacy_benefit_managers.shtml)
[4] [webpage](http://tsi.brooklaw.edu/cases/muecke-company-inc-v-cvs-caremark-corporation)
[5] [webpage](http://www.jdsupra.com/post/documentViewer.aspx?id=34954c00-b2a2-4299-9699-6a5a61e7a242)
[6] [webpage](http://www.usatoday.com/money/economy/2008-11-14-1465930038_x.htm)
[7] [webpage](http://www.mbo.ca.gov/consumer/access_records.html)
[8] [webpage](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/medicalrecords.html)
[10] [webpage](https://www.privacyrights.org/Credit-and-Credit-Reports)
[11] [webpage](http://www.privacyrights.org/fs/fs8-med.html)
[12] [webpage](http://www.hmisters.com/contact_us.html)
[13] [webpage](http://www.ingenix.com/contact-us/inquiries/)
[14] [webpage](https://secure.medicalletter.org/)
[15] [webpage](https://www.supremecourt.gov/opinions/10pdf/10-779.pdf)
[16] [webpage](https://docs.google.com/viewer?a=v&q=cache:hviByfvPIyQJ:citeseerx.ist.psu.edu/viewdoc/download%3Ffmt%3Dpdf%3D1.1.125.980%26rep%3Drep1%26type%3Dpdf&hl=en&gl=us&pid=bl&srcid=ADEGEgsveyulSNdZv7CNyf0dq8NUd6y7TvTvdPQYBXflbx_BnHu7lyphaxXcbXUc_ZZhzU013CFyBRTvqz986o5w9wGdwxr cynl5G&amp;sig=AHEtbTQhvZ_g999 EqpHChkoGLUTZ0sNyDw)
[18] [webpage](http://totalcapitol.com/?bill_id=200920100AB2112)
[20] [webpage](http://www.opp.usdoj.gov/BAU/) todayPMIX.pdf
[22] [webpage](https://epic.org/privacy/individuals/)
[23] [webpage](https://docs.google.com/viewer?a=v&q=cache:hviByfvPIyQJ:citeseerx.ist.psu.edu/viewdoc/download%3Ffmt%3Dpdf%3D1.1.125.980%26rep%3Drep1%26type%3Dpdf&hl=en&gl=us&pid=bl&srcid=ADEGEgsveyulSNdZv7CNyf0dq8NUd6y7TvTvdPQYBXflbx_BnHu7lyphaxXcbXUc_ZZhzU013CFyBRTvqz986o5w9wGdwxr cynl5G&amp;sig=AHEtbTQhvZ_g999 EqpHChkoGLUTZ0sNyDw)
[25] [webpage](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=11001-12000&file=11053-11058)