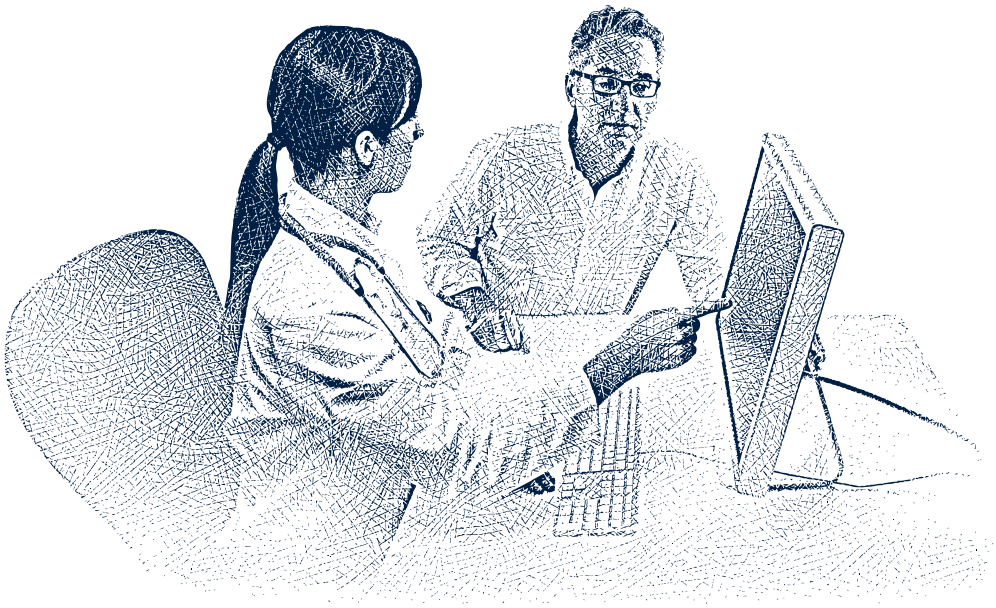

Health Records Privacy in California

Protecting your privacy as patient records go digital

This fact sheet provides an introduction to electronic health records and your medical privacy rights. To learn more, refer to the companion resource, Health Records Privacy in California: Answers to Frequently Asked Questions, which provides additional information in a Q&A format.

A Consumer Action Publication

www.consumer-action.org

When you visit a doctor, fill a prescription, get an X-ray or have a blood test, you want to be confident that your personal health records will remain private unless there is a legitimate medical or business reason for using them. Over the years, many safeguards have been put in place to prevent unauthorized access to patient information, including some that address recent changes in how personal health information is collected, managed and shared.

As the country moves from paper files to digital medical records, it's important to be aware of both the benefits and the potential risks of electronic file sharing, and to understand your medical privacy rights and what steps you can take to maintain the confidentiality of your health records in any format.

Health information technology

Health information technology makes it possible for your doctor, other health care providers, a hospital, medical labs, health insurance claims processors and others to use computers to create, store and share your health information electronically. Storing and sharing digital personal health files has the potential to:

- make nearly instant retrieval of all your critical health information possible, even when you are far from home;
- greatly reduce the chances of different doctors prescribing incompatible drugs or duplicating tests;
- eliminate errors due to illegible handwriting;
- protect records even during a disaster, when paper files could be destroyed or inaccessible;
- enable patients to view test results and personal health information online; and
- limit who can view records (through encryption and password protection) and track who has accessed patient files.

New privacy risks

Along with these and other potential benefits come some new privacy risks. Because digital health records bring together so much information (personal data, payment details and medical notes) and enable so many patients' files to be stored in one place, a single instance of unauthorized access (data breach) could threaten a huge number of electronic records and be particularly damaging to the individuals affected.

A breach can be accidental, such as when an employee mistakenly uploads

unencrypted patient records to the Internet. Or it can be intentional and criminal. Stolen information can be used to commit credit card fraud or to obtain medical services under other people's health plans.

Breaches aside, marketers, fundraisers and pharmaceutical companies who obtain your information can use it to sell you products and solicit donations.

Your medical privacy rights

Regardless of format (paper or electronic), it's important to understand how the law protects—or doesn't protect—your medical information.

The main federal law governing the collection, storage, use and disclosure of "protected health information" is the Health Insurance Portability and Accountability Act (HIPAA). (Protected health information includes at least one element, such as a name, address or Social Security number, that could be used to reveal your identity.)

While HIPAA generally applies to health records in any format, the HIPAA Security Rule applies specifically to electronic records. It requires covered entities to implement appropriate safeguards to protect the privacy of patients' information held in digital format.

A HIPAA-covered entity is any health care provider (doctors, nurses, hospitals, pharmacists, dentists, etc.), health plan (including HMOs and programs such as Medicare) or health care clearinghouse that transmits claims, billing and other patient information. Other individuals and businesses that contract to provide services for covered entities generally must comply with HIPAA's rules, too.

States can create stronger (but not weaker) rules to protect patient privacy.

California residents are protected by federal laws as well as some even stronger state regulations. Under HIPAA, California's Confidentiality of Medical Information Act (CMIA) and other state laws, you have the right to be informed. Health care providers must give you a Notice of Privacy Practices, which clearly explains how your protected health information may be used, who could see it, what your rights are and where to complain.

Signing the Notice of Privacy Practices means only that you received and understand it, not that you authorize any use or disclosure of your health information for other than routine purposes (health care providers can use and disclose your protected health information for treatment, payment and health care operations—administrative services—without first obtaining your signed permission) or those allowed by law.

If your provider uses an outside service to send and receive digital health records, you may be given a chance to either "opt in" or "opt out" of electronic records sharing. Under an opt-in consent policy, you are asked to sign a form giving or refusing your permission. Under an opt-out consent policy, your

agreement is automatic unless you, within a certain time, deny permission by submitting a form.

You can't be denied medical care or insurance or otherwise penalized because you say no to electronic sharing of your information when given the choice. However, your "opt out" could be ignored in a medical emergency or public health crisis.

Protecting your medical privacy

While some uses of your information are out of your control, there are steps you can take to improve the privacy and security of your health records.

Understand what you're signing. Read medical records release authorization forms carefully. If you don't understand something, ask for an explanation. Don't sign broad or vague authorizations. If necessary, edit the form by crossing out the language you don't agree with and writing in specific restrictions and time limits. Initial your changes.

Discuss your privacy concerns with your provider. Electronic health records can offer better security options than paper files, such as encryption (making them unreadable to unauthorized users), electronic tracking (recording who accesses the file and what changes are made) and security access settings (passwords and PINs). Ask your provider how it prevents unauthorized access.

Request a restriction. If you don't want a certain treatment, medical condition, visit, etc. disclosed, even for routine purposes, send a written request to your provider. A health care provider is not required to agree to a restriction, but if it does, it must not use or disclose the restricted information unless it is needed to treat you in an emergency. If your request is denied, ask for an explanation.

Don't answer off-topic questions on forms. If you're seeking care for a sprained wrist, it is unlikely your provider needs to know whether you smoke. If an answer is really needed, the provider will ask you.

Be careful when sharing with non-providers. Many medical privacy laws apply only to health care providers and other "covered entities." When you participate in health surveys and free or low-cost health screenings, sign up online or offline to receive free samples, use health and fitness "apps" on your mobile device and visit online health websites and forums, you can't control who sees the information you provide. Read the company's privacy policy (websites and mobile apps that collect personally identifiable information from Californians are required to have a privacy policy that is easily accessed by consumers) and any authorization forms before revealing anything. Do not download an app until you understand what information it will collect and how it will use and share it.

Limit who sees your information. Health care providers can use and disclose your information as needed, without your written permission, for treatment, payment and administrative purposes.

Generally speaking, any other use of your protected health information not specifically allowed or required by law (for law enforcement and public health purposes, for example) requires your written "authorization" (often referred to as "consent" in California.)

A valid authorization must specify what health information can be shared, who is authorized to disclose and receive the information, the purpose of sharing the information, and an expiration date.

You have rights regarding the use and disclosure of your information.

Withhold your consent or authorization. You are allowed to refuse to share your information with any third party. If you pay by cash, you can instruct your provider not to share information about your treatment with your health insurance plan.

Revoke your consent or authorization. You can cancel your permission to disclose your health information (paper or electronic) at any time. You can also give permission if you previously denied it.

If you withdraw consent to exchange your information electronically, any health information shared electronically up to that time will continue to be stored digitally, but it will not be accessed that way for future treatment.

Know who has seen your information. Upon your request, your health care provider must give you an "accounting of disclosures," which is a list describing how your health information has been shared for purposes other than treatment, payment and health care operations in the previous six years. You should receive the report within 60 days of your request.

You also must be notified of a security breach of your unencrypted electronic health information. In California, the notice must include the type of information breached, the time of the breach and the toll-free phone numbers and addresses for the major credit reporting agencies.

Stop receiving marketing messages. Health care providers are not allowed to give or sell your information for direct marketing purposes without your signed authorization. They must clearly tell you how the information will be used and whether they will be paid for providing it. You also have the right to opt out of a provider's fundraising messages.

Your health plan is still allowed to send you information about its own health care services, including treatments and drugs, without your written permission.

Your medical records

A doctor or health plan must allow you to view your health records during business hours within five working days of receiving your written request. California law allows providers to charge for clerical costs related to making patient records available.

Copies you request must be provided within 15 days, or 10 days if you agree to receive a summary of your records. In California, providers are allowed to charge up to 25¢ per page for photocopies or 50¢ per page for copies from microfilm, plus a "reasonable" fee for administrative costs in making your records available to you, and postage if you have the copies mailed. The fee for copies of X-rays and similar records must be based on the actual cost of copies.

Since most medical records contain many pages, consider requesting copies of just those items you need rather than the entire record. If your health record is held digitally, receiving the information on a CD, DVD or Internet download saved to a USB flash drive may be cheaper and more convenient for you.

You are entitled to a free copy of the relevant part of your medical record if the information is needed to appeal a denial of eligibility for public benefits such as Medi-Cal and Social Security disability. If your appeal is successful, your provider can then charge you for the copy.

If you feel you're being overcharged or you are having difficulty getting your records, contact the Medical Board of California (www.mbc.ca.gov) to complain and get assistance.

In California, you can be denied access to your mental health records if the provider believes that seeing the record might be harmful to you or someone else. You can also be denied access to information that someone who is not a health care provider gave about you in confidence if disclosure would reveal that person's identity. If you are denied access to a portion of your records, you must be given the reason, and you must be told if you have a right to have the decision reviewed and how you can file a complaint.

Make changes to your medical records. You can ask for a change to your medical records if the information is incorrect or incomplete. If the provider believes the information is accurate and complete and won't make the change, you can add a 250-word statement of disagreement to your file.

When your medical privacy rights are violated

If you believe that your medical privacy rights have been violated, start by filing a complaint directly with your health care provider. The Notice of Privacy Practices you received must include information about how you can file a complaint. Under federal law, a covered entity cannot retaliate against you if you complain.

Separate state and federal laws cover privacy violations, so if you escalate your complaint beyond your provider, you may have to register complaints with more than one agency.

HIPAA-covered entities. For violations by HIPAA-covered entities or their business associates, you can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights (OCR): www.hhs.gov/ocr/privacy/hipaa/complaints. Use the OCR's complaint package (www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf), which includes information on where to mail your complaint form. For more information, call 800-368-1019 (TDD: 800-537-7697) or email OCRComplaint@hhs.gov.

Health plans and HMOs. The California Department of Managed Health Care handles patient complaints regarding health plans and HMOs: www.hmohelp.ca.gov/dmhc_consumer/pc/pc_complaint.aspx. For urgent complaints, call 888-466-2219 (TDD: 877-688-9891). For complaints that aren't urgent, fill out and mail a complaint form: www.hmohelp.ca.gov/dmhc_consumer/pc/pc_forms.aspx.

"Division 2" facilities. The California Department of Public Health Licensing and Certification Division investigates complaints involving clinics, acute care hospitals, skilled nursing facilities, correctional treatment centers, home health agencies, hospices and mobile care units. To find the nearest District Office, visit http://www.cdph.ca.gov/certlic/facilities/Pages/LCDistrictOffices.aspx.

Other providers and businesses. To report a medical privacy or security violation by any other type of provider or person, file a complaint with the District Attorney of the county in which the incident occurred (www.cdaa.org/district-attorney-roster).

Medi-Cal beneficiaries. If you receive Medi-Cal benefits, you can report your complaint to the California Department of Health Care Services (916-445-4646; www.dhcs.ca.gov; privacyofficer@dhcs.ca.gov).

General privacy complaints. The Federal Trade Commission takes legal action against organizations that violate consumers' privacy rights or fail to maintain security for sensitive consumer information. Learn more or file a complaint: www.ftccomplaintassistant.gov.

Legal action. Californians can sue a person or entity that negligently releases confidential information or records in violation of California law—not an option under federal law. Contact the California Attorney General's office (800-952-5225; www.oag.ca.gov) or your district attorney (www.cdaa.org/district-attorney-roster). You can also view and search a list of data breaches on the AG's website.

Consumer Action

www.consumer-action.org
San Francisco, CA
415-777-9635
info@consumer-action.org

Los Angeles, CA
213-624-8327
outreach@consumer-action.org

Washington, DC
202-670-3601
dc-office@consumer-action.org

Consumer advice and referral hotline

Submit consumer complaints about consumer problems to our advice and referral hotline:
http://www.consumer-action.org/hotline/complaint_form/
or 415-777-9635.

Chinese, English and Spanish spoken

Consumer Action created this brochure under a grant from the Rose Foundation.
Consumer Action empowers low- to moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. To learn more, visit www.consumer-action.org.