Privacy Protections for Medical Information in Government, Research, and Public Health Records (California Medical Privacy Series) [1]

1. What does this guide cover?

It's common to think about your medical information only within the context of your own health care. However, medical information can circulate well beyond treatment while still falling within the protection of the law. Alternatively, there are many situations where health privacy or other privacy laws will not apply. This guide covers some of the less obvious protected and unprotected uses of medical information, including:

- public health reporting,
- national security,
- public records,
- health and medical research, and
- government benefit, discount, and license programs.

2. Medical information collected for public health purposes

The primary federal law that protects the privacy of medical information is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In California, the Confidentiality of Medical Information Act (CMIA) offers additional protections. Both HIPAA and California law attempt to balance individual privacy rights with the need to protect public health.

Public health authorities (such as the Centers for Disease Control and Prevention, the Food and Drug Administration, and your state and local health departments) and other government agencies (such as law enforcement) monitor disease and health safety issues. They also intervene on behalf of the public in certain situations, for example, epidemics, outbreaks of food-related illness, and natural disasters. To carry out their functions, they need access to individual medical information.

a. Types of public health reporting

i. Mandatory reporting

There are times when health care providers are required by law to report health and medical information. Federal and state government agencies need this information to monitor community health at local, state, and national levels. In addition, agencies use the information to monitor and measure the effectiveness, accessibility, and quality of available health services.

Under federal law, some examples of mandatory reporting include: births and deaths; child or elder abuse; treatment of gunshot or knife wounds; industrial accidents; and data required for public health surveillance, investigations, or interventions. 45 CFR §
The California Department of Public Health website links to several lists of mandatory Reportable Diseases and Conditions in the state.

If you are interested in the history of mandatory public health reporting, see Appendix A of the American Health Information Management Association (AHIMA) publication, Mandatory Reporting—Balancing Patients’ Rights with Public Health Interests.

i. Permitted (or notifiable) reporting

There are times when covered entities may disclose information without your authorization to support public health surveillance. Officials request that healthcare providers report information so they may detect unusual occurrences of diseases, monitor trends, and evaluate the effectiveness of interventions.

The Centers for Disease Control (CDC) publishes the Morbidity and Mortality Weekly Report (MMWR) about health and behavioral trends and statistics. The CDC website has more information on the National Notifiable Diseases Surveillance System, which enables public health agencies that range from local to international to share what’s reported about notifiable diseases. This helps public health officials to monitor, and ideally, to prevent the spread of diseases in this category. The current and historic list of notifiable (permitted) diseases to be reported is here.

One example of public health reporting for health surveillance is disease registries that provide epidemiological data such as the National Cancer Institute’s Surveillance, Epidemiology, and End Results (SEER) program. It collects cancer data from around the U.S. in order to:

- estimate regional cancer trends and mortality rates;
- identify unusual appearances of or changes in certain forms of cancer in population subgroups;
- produce current information on clinical presentation (what makes a cancer identifiable) and modifications in therapy and their effect on survival; and
- promote studies to identify when cancer control interventions, such as recommended screening practices like a colonoscopy, prostate exam, pap smear, or mammogram, may or may not be effective.

A public health disclosure of individual health information may also occur when a health care provider is legally authorized to notify individuals at risk of contracting or spreading a disease or condition. For example, an individual who tests positive for HIV will be asked for names of others whom he or she might have exposed to the disease. The provider will notify those individuals.

45 CFR § 164.512(b)(1)(iv) [2]

Under California law a physician who reports a patient’s positive HIV test results to someone she believes is the patient’s sexual partner, or with whom she believes the patient has shared needles, may not be held liable for the disclosure. Cal. Health & Safety Code § 121015 [9]

b. Does the law protect your health information when it is used for public health purposes?

The answer is that it really depends on whom your health care provider shares the information with. The notice of privacy practices you receive from your health care provider will inform you that the provider does not need to get your written permission to disclose your information for public health purposes.

If the public health authority that receives your information is also a covered entity, the HIPAA Privacy Rule will apply. 45 CFR § 164 [2]

If it is not a covered entity, the public health authority’s data practices will be subject to whichever laws, regulations, and policies apply to it. For example, if the Food and Drug Administration (FDA) receives information on salmonella cases from health care providers, the laws and regulations governing the FDA’s privacy and security practices will apply rather than HIPAA. 21 CFR, Part 21 [10]

Unless specific rules and regulations govern the privacy practices of a public health authority receiving your information, the only privacy protection built into public health reporting is the minimum necessary standard. In other words, covered entities are supposed to limit the information they disclose to public health authorities to the minimum amount necessary to accomplish the public health purpose.

Health care providers may develop their own policies and procedures for the minimum necessary information required for a specific purpose. Examples of mandatory disclosures where the "minimum necessary" may apply are:
• births and deaths (reported to state vital statistics agencies);
• gunshot wound treatment (reported to law enforcement);
• suspected child and elder abuse (reported to law enforcement and social welfare agencies);
• industrial accidents (reported to CalOSHA); and
• certain poisonings, abortions, cancer cases, and communicable diseases.

When a public health authority requests information—for example to monitor a disease outbreak or investigate a food or product safety issue—it determines the minimum necessary information it needs. 45 CFR § 164.514(d)(3)(i) [11]

c. Public health reporting and health information exchange (HIE)

The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires health care providers to begin implementing electronic health record systems (EHRs) and start meeting public health reporting requirements electronically. 42 U.S.C. § 139 w-4(o)(1)(A)(i) [12]

This information may include laboratory, immunization, and syndromic surveillance reports. Syndromic surveillance means using real-time medical data to anticipate the outbreak of a disease and mount a public health response, even prior to an actual diagnosis. One example is Influenzanet [13], a Europe-wide system based on voluntary reports of the presence or absence of flu symptoms on the internet. Among other things, it allows for early warnings of flu trends and enables people to take precautions.

Electronic health information exchange (HIE) makes it easy to collect large amounts of data. As it becomes easier and more efficient to collect and share health information, public health organizations will likely have unprecedented access to population health data. With this access, the organizations may have the opportunity to use data in new ways.

With HIE, public health organizations may also be able to enhance their existing data uses, such as:

• addressing disparities in population health and in health care delivery—for example, between urban and rural health care delivery, or differences by race, ethnic group or income level;
• improving care for chronic diseases like cardiovascular disease, asthma, and diabetes;
• improving public health surveillance in ways such as better monitoring of flu epidemics and verifying whether vaccines are working;
• improving monitoring of priority public health issues such as cancer screening (for example, measuring the impact of mammograms, colonoscopies, and prostate exams on disease rates) and diabetes (tracking individually identifiable lab results for blood sugar and kidney function, which is already being done with syndromic surveillance reporting in New York City, and in a number of other statewide or county level programs);
• expanding disease registries to produce better statistical information (for example, for screening and managing chronic diseases like diabetes and AIDS);
• communicating public health alerts.

As electronic reporting generates more data, public health organizations and private researchers may start asking for more access to the information. For instance, public health agencies may want to expand the lists of mandatory and permitted reportable information and expand access to this information.

If, or when, this happens, the question arises as to whether these agencies must publish notices of any proposed changes in the Federal Register[14] and solicit public comment. Because the reporting regulations are already codified, modifying them should require public notice and comment. 45 CFR § 164.512 [11] (Unfortunately, the Federal Register is not the most user-friendly document or website, so you may want to periodically ask your health care provider if and how her reporting requirements have changed).

3. Medical information collected for national security purposes

Regardless of whatever laws protect the privacy of health information, the U.S. government may access any information it deems necessary to protect the security of the nation. Two laws passed in the aftermath of the September 11, 2001 terrorist attacks codify the government’s authority to access any and all information needed to carry out its mission: the Patriot Act (Public Law 107-56, 115 Stat. 272 (2001) and the Homeland Security Act (Public Law 107–296. 116 Stat. 2135 (2002). The Patriot Act reduces (some would say eliminates) restrictions on law enforcement requests for health records, as well as communications records, including email and phone records. Section 215 of the Patriot Act gives the FBI director authority to apply to the secret FISA (Foreign Intelligence Surveillance Act) court for an order that a person or entity produce “any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine
intelligence activities.” The Homeland Security Act created the Department of Homeland Security. The Act gives the department’s secretary the authority to conduct the investigations necessary to preventing foreign and domestic terrorism, and to access the information needed to do so. These acts and their broad powers override the privacy protections of lesser laws, like HIPAA.

4. Medical information gained through government records requests

The Freedom of Information Act (FOIA) is the federal law that allows individuals to request access to government records. [5 U.S.C. § 552] [15] There are nine exemptions to FOIA, including one for medical records: “personnel and medical and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” [5 U.S.C. § 552(b)(6)] [15] This means that if a government agency has your medical records because, for example, you are a patient at a Veterans Administration hospital, or you participate in an AIDS study at the National Institutes of Health (NIH), the agency may not release your records to a FOIA request from anyone other than yourself. If someone else makes the request (for example, a reporter or media organization) and it is denied and goes to court, the court must balance the public interest in disclosure against your personal privacy interest.

California’s Public Records Act (Cal. Gov’t Code § 6250, et seq [16]; also known as the Brown Act) is similar to FOIA. It too exempts medical records held by government agencies from disclosure requests. The Brown Act incorporates California’s patient-physician privilege law (Cal. Evidence Code §§ 990–1007 [17]), the Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56–56.37 [18]) and the HIPAA Privacy Rule (45 CFR § 160 [19] and Subparts A and E of § 164 [2]). As with FOIA, even with the medical records exemption, the agency or court deciding what information may or may not be released must balance individual privacy against the public’s right to know. To learn more about the California Public Records Act, see The People’s Business: A Guide to the Public Records Act [20], published by the League of California Cities [21].

5. Medical information disclosed for research purposes

HIPAA and the CMIA both address how medical information may be shared and used for research purposes. However, different laws will apply when research is conducted on human subjects because of the ethical concerns it raises.

a. HIPAA

HIPAA requires researchers to obtain authorization to use your identifiable medical information for research purposes. You must give your signed permission stating that the researcher may use your information, but only for a specific project described in the agreement and only until the project's stated expiration date.

Researchers may obtain a single authorization for both "conditioned" research (where treatment in a clinical trial is conditioned on receiving your authorization) and "unconditioned" research (research not related to treatment). An authorizations may be for a specific study, or it may encompass a range of future research projects. Any authorization you are asked to sign for future projects must adequately describe the nature of the research that will be undertaken.

You may have additional protections when researchers use your identifiable information, but it will depend on specific regulations governing the agency responsible for the data. For example, the Agency for Healthcare Research and Quality (AHRQ—a part of the U.S. Department of Health and Human Services) [22] funds and oversees a great deal of health research by public and private organizations. AHRQ, its contractors, and its grantees may only use identifiable data for the specific purpose to which you have consented. [42 U.S.C. § 299c-3(c)] [23]

Your medical information may be used for research without your consent in the following situations:

- The medical information has been de-identified according to HIPAA standards. This means that 18 specific identifiers [24] have been removed—including name, Social Security number, photos, and unique characteristics. When information has been de-identified according to this standard, there are no limits on how it may be used and disclosed. [45 CFR § 164.514] [19] However, there is nobody certifying or monitoring whether the standard has been met.

- It is a limited data set, meaning that most identifiers are removed. However, a limited data set may still include dates of admission or discharge from a hospital; dates of medical treatment; date of birth and death; age (including 90 or older, which would limit the population pool from which the data could be re-identified); and a five-digit ZIP code, along with state, county, city, or precinct, but not your actual street address. The researcher and your health care provider—but not you—must also have a written agreement that covers all permitted uses of the data. [45 CFR § 164.514] [19]

- An Institutional Review Board (IRB) (an independent ethics board; although it depends on where the research is being conducted, an IRB is usually composed of medical faculty at the research institution) or Privacy Board has determined that
the project presents minimal risk to privacy, that procedures are in place to protect identifiable information, and that the research could not be done without identifiable information. 45 CFR § 164.512(i)(1)(i) [19]

See the HHS publication Research [25] for more information on how the HIPAA Privacy Rule applies to research.

b. CMIA

California's Confidentiality of Medical Information Act (CMIA) allows disclosure of individual medical information for bona fide research purposes to public agencies, clinical investigators (including those conducting epidemiologic studies), health care research organizations, and accredited public or private nonprofit educational or health care institutions. The CMIA prohibits disclosure beyond the purpose of the research in any way that would reveal the identity of a subject. Cal. Civ. Code § 56.10(c)(7) [18]

c. Research on human subjects

Research that is conducted on human subjects is another matter. Separate federal regulations govern biomedical and behavioral research ethics. These include The Common Rule and the Food and Drug Administration's (FDA) regulations on protecting human subjects. The Common Rule, 45 CFR § 46(A) [26]; the FDA regulations are at 21 CFR §§ 50, 56 [27]

The Common Rule came into being primarily in response to the revelation that African-American men were the unwitting subjects of the federally funded Tuskegee Experiment, conducted from 1932–1972 by the U.S. Public Health Service to study the effects of syphilis. The study monitored 600 low-income African-American men, of whom 400 were infected with syphilis, for 40 years. They were never told they had the disease, and were not treated with penicillin when it became available in the 1950s. After the existence of this study was revealed, public outrage and political embarrassment finally forced the Public Health Service to end it.

Research on human subjects now requires authorization and informed consent. In other words, you must sign an agreement and have the information you need to understand the research project. In particular, you must understand the risks and benefits of the project.

An informed consent agreement must tell you:

- the purpose of the research;
- the procedures involved;
- alternatives to participation (for example, is there a non-experimental drug or treatment available for the condition being studied?);
- all foreseeable risks and discomforts, including physical injury, and possible psychological, social, or economic harm, discomfort, or inconvenience;
- possible benefits of the research to you and society;
- how long you are expected to participate;
- a contact for answers to questions and in case of a research-related injury or emergency;
- that participation is voluntary and there are no consequences or possible loss of any benefits you are entitled to receive if you do not participate;
- your right to confidentiality; and
- your right to withdraw at any time without consequences.

An IRB, also known as an independent ethics board, may waive one or more of these requirements if it would make the project impractical or impossible to do. An IRB may also waive a requirement if it does not apply to a particular project.

The California Attorney General's Office has an Experimental Research Subject's Bill of Rights [28] that replicates the federal informed consent requirements. Also see Cal. Health & Safety Code § 24172 [29]

If you ever consider participating in a medical study or clinical trial, you may want to read more about how your information may be used and any rights you have. HHS has a publication on the Common Rule as it applies to research titled Federal Policy for the Protection of Human Subjects ('Common Rule') [30]. Fifteen government agencies, including the departments of Veterans Affairs, Defense and Education have signed on to the Common Rule; the CIA, Homeland Security and the Social Security Administration are also bound by the Rule although they have not signed on.

The National Institutes of Health (NIH) compares the HIPAA research requirements to the HHS and FDA regulations for the protection of human subjects: How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule [31]? [31] The University of Southern California also has a publication titled Informed Consent in
d. Precision Medicine Initiative

In his 2015 State of the Union address, President Obama announced the Precision Medicine Initiative (PMI). The project’s goal is to advance the treatment and prevention of disease and change the medical practice model of “one size fits all” to individually targeted designer medicine. The first step is to build a nationally accessible electronic archive by 2020 that includes individual whole-genome sequencing, behavioral and environmental data, and all electronic health records of 1 million or more Americans who volunteer to participate.

The research that will be based on this data requires participants to consent to its use by researchers in both the public and private sectors, which will most certainly include drug and medical device manufacturers. This will mean changing current regulatory schemes that exist to protect health privacy and uses of health information. The National Institutes of Health (NIH) is working with the Department of Health and Human Services (HHS) to bring the Common Rule (see 5c, “Research on Human Subjects,” above), a decades-old rule originally intended to protect research participants, more in line with PMI participants’ desire to be active partners in advancing modern medical science. The PMI is intended to drive innovation, while also building public trust that the technologies and treatments it develops are safe and effective, and that the highest standards of privacy and security are in place. Given the quantities of personal and medical data involved, and the emphasis on allowing data to flow freely and quickly to qualified researchers, it is hard to envision just how the PMI will maintain privacy and security.

In any case, participants will be asked to voluntarily give up the limited protection of their PHI that HIPAA and the CMIA afford. They will consent to extensive characterization of their biologic specimens—cell populations, proteins, RNA, and DNA—as being, for example, susceptible or resistant to certain diseases or conditions, either by themselves or in combination with other factors. The data could also include whole-genome sequencing, although at a cost of $1000 per person, the first round of PMI funding—$215 million—is unlikely to cover it (assuming that Congress funds the PMI at all). Behavioral data (records of mental health and substance abuse treatment) and environmental data (which may mean a participant’s exposure to known toxins, such as chemicals used in dry cleaning or in beauty salons) will be open to researchers, and all new, PMI-generated data, along with pre-existing data, will be linked to participants’ electronic health records.

An important aspect of the PMI will be pharmacogenomics, the study of how our genes affect our response to drugs, since a major goal of the initiative is to optimize the usefulness of drugs in the treatment of diseases. Research will be focused on delivering the most appropriate and effective drug, in the right dose, to the right patient. Doctors will certainly be interested in the outcomes of pharmacogenomics research, and pharmaceutical companies will be no less interested. In fact, they will undoubtedly be involved in the research and will have access to patient-participants’ complete medical, genetic, behavioral and environmental data. It would seem to go without saying that clear restrictions on the uses of personally identifiable data by profit-making research entities (as well as hybrid research entities that include profit-making companies), that include auditing and enforcement, be in place before the PMI starts collecting data and making it available.

The possibility of more effective treatment of many chronic and fatal diseases by changing the research and treatment paradigm is something to raise everyone’s hopes. There seems, though, to be considerable risk of privacy getting lost in the excitement about the treatment breakthrough possibilities and the seismic shift in the way medicine is practiced that the PMI portends. PMI research envisions public-private partnerships. In view of that collaboration, it is very important to prevent participants’ medical and genetic information from being exposed to the ruthless and insatiable world of commercial data mining.

6. Medical information disclosed to receive a public benefit, discount, or license

Many public agencies offer discounts and special benefits to disabled individuals. These might include transit passes, hunting and fishing licenses, and state park admission passes, among many others. To qualify, an applicant generally must fill out an application that summarizes (sometimes from a checklist, sometimes in writing) the impairment that entitles him or her to a discount or service, and he or she must have a licensed health or behavioral practitioner sign to certify the claim.

Some California benefits, for example to receive a disabled parking placard [34], require additional descriptive information about the qualifying disability from a health care practitioner as part of the application.

a. Information you provide to a California state agency

As long as the information is provided to a state agency, it is protected by California’s Information Practices Act (IPA). Cal. Civ. Code § 1798 et. seq [35]. This act protects personal privacy by limiting how much information an agency can collect, maintain, and distribute. It gives you the right to review your personal information in state agency records, request changes to inaccurate or irrelevant information, and obtain an accounting of who has accessed the information. The IPA allows anyone other than
yourself very little ability to access your personal information.

b. Information you provide to a local government agency

The IPA does not apply to local government agencies. If you apply for a disability-discounted transit pass for your local public bus service, the privacy of your medical information depends on the city or county's general privacy policy, or the policy of the agency itself—if it has one.

c. Information you provide to a private business or nonprofit

If you apply to a private business or nonprofit for a benefit or discount based on a disability, the privacy of any medical information it collects from you depends on the policy of the company or organization, unless other laws apply. If you must give up medical information to obtain a benefit or discount, it is always a good idea to ask what privacy protections apply to the information, if any.

7. Additional Resources

Federal laws and resources

U.S. Department of Health and Human Services
Office for Civil Rights [36]

The full text of the Privacy Act of 1974 is available here [37].

Centers for Disease Control and Prevention [38]

California laws and resources

To find the full text of California laws, visit California Legislative Information [39].

California Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56-56.37)

California Department of Public Health: Reportable Diseases and Conditions [3]

California Health Benefits Exchange: Covered California [40] [41]

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
[10] https://www.ecfr.gov/cgi-bin/text-idx?SID=bef6793bd9f9a357f23e34295009a96b&amp;mc=true&amp;tpl=/ecfrbrowse/Title21/21tab_02.tpl
SID=198ca14854a303fb0e349e775449aeb4&amp;mc=true&amp;tpl=/ecfrbrowse/Title45/45tab_02.tpl