**Personal Health Records and Your Privacy (California Medical Privacy Series)**

[1]

1. What does this guide cover?
   
   This guide provides general information about personal health records (PHRs), highlights privacy concerns, and points out existing privacy protections.

2. What are personal health records and what information do they contain?

   A personal health record (PHR) allows you to store, manage, and share your medical information. The California Attorney General’s Privacy Protection and Enforcement Unit defines PHRs [2] as “Internet-based applications that allow you to gather, store, manage and, in some cases, share information about your health or the health of someone in your care.”

   It’s likely you have many different health care providers and you may have records at a hospital, a physician’s office, dentist, pharmacy, and an optician. You also have the right to access your medical information. PHRs allow you to gather information from multiple sources and keep your medical history as a single record. PRC has a sample letter [3] for requesting copies of your medical records.

   The ability to manage your own health information is one factor that distinguishes a PHR from an EHR (electronic health record). An EHR is one of many individual records contained in an electronic records system that your health care provider controls and populates with information.

   With a PHR, you have control over the information you enter, and can decide how you share with others. However, this does not mean that you have complete control over who can see your medical records or how they are used. Those records all exist elsewhere, in either paper or electronic form, under the control of your health care providers. Both federal and state laws govern what health care providers can do with your personal health information (PHI). See the HIPAA Privacy Rule at 45 CFR Part 160 [4] and Subparts A and E of Part 164 [5] and the Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code §§ 56–56.16 [6].

   The features that PHRs offer vary, but many have the ability to store and transmit:

   - information about your medical history;
   - information about your prescriptions, including dosages and refills;
   - diagnostic test results, both laboratory and imaging;
   - drug alerts;
   - immunization records; and
   - physician treatment plans.

   A PHR may also support options such as secure email with your physicians and links to medical informational websites and archives.
3. What types of personal health records are available?

PHRs can be paper based or electronic. Electronic records can be kept on different media, including personal computers and smart phones, smart cards, thumb drives, CDs, or web-based applications. Of the two types, paper records may be easier to secure, but electronic records are more convenient. They are easier to update and maintain and also easier to access and share.

- **Paper.** You may already have your own paper-based PHRs—folders filled with records from doctors, pharmacies, hospitals, and insurers. These may include copies of diagnostic test results, drug notices that accompany prescriptions, or treatment invoices and Explanations of Benefits from providers and insurers. Also, you may have begun to receive a clinical summary print-out of your visit when you leave your doctor’s office that you can put in your folder of paper records. Giving patients this information is one of the requirements health providers must meet in the step-by-step progress to achieving “meaningful use” (the HITECH Act’s term) of electronic health records in their practice. A folder with all of this information—locked in a secure filing cabinet—offers a good, if limited, snapshot of your medical history. What it lacks is easy accessibility by others. For instance, if you want to share lab test results between doctors, you will need to copy a form and fax or mail it, scan and email it, or carry hard copies around with you.

- **Personal Computer.** You can install a PHR application on your computer where you may input information, download files, and scan documents you receive from your healthcare providers. The information is stored locally on the computer, on a CD, on a thumb drive, or on another storage device. You control it and have the ability to update and print it. However, if you have a medical emergency, nobody will be able to access your medical history through your PHR unless you carry an up-to-date CD or thumb drive with you and can tell the ER staff where it is—and they have a means of reading it.

- **Internet.** Most PHR products are Internet based—similar to a local application on your computer, but accessible online when you log in with a user name and password. Microsoft’s HealthVault [7] is an example of this type of PHR. An online PHR lets you manage your records from wherever you are—you can update and transmit the information, and give others access.

  Internet-based PHRs make your medical information available in non-emergency situations, and also in emergencies as long as you’re able to provide your user name and password.

  The security of an internet-based PHR depends on the security of the devices you use to store and transmit your information, whatever is built into the PHR application itself, and the security of the network. A good question to ask if you’re considering this type of PHR is whether the data is encrypted where it is stored and also when it is in transit.

- **Mobile applications.** Apps are becoming the default Internet-based PHR application, in part because they are extremely convenient.

  Mobile PHR apps have a variety of different features. For example, you can maintain and manage your medical information. You can also send information and receive medical information from health care providers and insurers. Because many smartphones have touch screens, an app may also be able to measure vital signs—like heart rate and blood pressure—and update your PHR continuously. Apps may even give you the option of sharing your data using social media.

  These apps present numerous privacy and security concerns. Again, you want to know about the presence or absence of encryption in applications and the networks over which they transmit data.

  The Food and Drug Administration (FDA) has developed guidelines for some types of mobile medical apps, but not those functioning solely as PHRs (see Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff [8]; note that the guidelines are non-binding). Only those that are either accessories to a regulated medical device (such as an app that monitors an insulin pump) or that transform a mobile platform into a regulated medical device (for example, an app that uses a phone’s touch-screen capability to monitor vital signs) are currently being considered for FDA regulation. For consumer information on the types of mobile medical apps the FDA takes an interest in, see Keeping Up with Progress in Mobile Medical Apps [9].

- **PHR smart card.** A number of vendors offer a secure PHR smart card that stores medical information. With the aid of a card reader, both you and your doctor can access your records on a computer screen and also update the card. Problems with this type of PHR may be how universally available card readers are and how secure the card really is, in case you lose it. Furthermore, it’s anyone’s guess who has adopted this type of PHR and the extent to which it is in use.

If you are considering using a PHR to maintain your health records, you may want to look at AHIMA’s (American Health Information Management Association) list of 12 Questions Consumers Should Ask When Choosing a PHR [10]. AHIMA also has
a website that can help you choose a PHR [11] based on your age and other health requirements. These questions cover issues of content, ownership and use of information, access and security, portability, and cost.

4. What privacy protections apply to PHRs?

The privacy protections that apply to PHRs depend on where the PHR originates. In general, this means that a PHR provided by your doctor or health plan is subject to more privacy laws than a commercial vendor that is not affiliated with your doctor or health plan.

A PHR that a doctor or a health plan provides is subject to laws that protect medical privacy and set security standards, including HIPAA and California’s Confidentiality of Medical Information Act (CMIA). HIPAA also imposes data breach notification requirements and penalties on this kind of PHRs.

California law may offer privacy protections for medical information in PHRs (even if they are not affiliated with your doctor or health plan). However, courts haven’t yet addressed this issue. The CMIA applies to “[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . . in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment or management of a medical condition of the individual.” Cal. Civ. Code § 56.06 [12]

For more information on medical privacy laws, see PRC’s guide: Health and Medical Privacy Laws (California Medical Privacy Series) [13].

a. When does HIPAA apply to PHRs?

For HIPAA to apply to a PHR, a HIPAA-covered entity must provide it. This generally would be a health care provider or a health plan that offers a PHR. If that is the case, the PHR comes under the federal privacy and security rules that protect your medical records.

This type of PHR is typically linked to the provider’s electronic health records (HER) system, and is sometimes referred to as a tethered PHR, although the PHR product itself may be offered and managed by a third party. The HIPAA term for a third party that performs services for a health care provider or health plan that require the use or disclosure of medical information is a business associate. Business associates are covered by the HIPAA, including the data breach notification requirements. A contract between a covered entity and a business associate spells out the business associate’s responsibilities with regard to the privacy and security of your health information that it handles.

Some common characteristics of this type of PHR include the following:

- It probably won’t give you access to all of the medical records your physician has for you, and may not automatically update your PHR. However, the PHR may give you the option to allow automatic updates.
- It probably won’t automatically link to or sync with PHRs you have with other providers. Even if you try to combine your information from multiple PHRs, you may find that the information is not available in a format that is fully compatible across PHRs.
- If your PHR allows you to enter your own information in your record and update it yourself, your entries will be distinguished from those a physician makes.
- Finally, a PHR that’s offered by a health care provider or health plan may not be portable, so it could be of no use to you if you change doctors or health plans—you would have to start over again.

The fact that HIPAA applies to a PHR gives you certain protections and rights. These are discussed in detail in the California Medical Privacy guide series: Health and Medical Privacy Laws [14]; How Is Your Medical Information Used and Disclosed [15]; Your Medical Information and Your Rights. [16] For a start, you must receive a notice of privacy practices informing you of protections and rights regarding your medical records. People often mistake this for a consent form, but it is not.

To summarize, the notice must:

- tell you how your doctor or health plan can use and share your medical records, and that your consent is not required to do this for purposes of treatment, payment, or health care operations;
- tell you that a provider or health plan is legally responsible for maintaining the privacy and security of your health information;
- inform you of your rights concerning your medical information—to access and copy your records and to amend them (which in reality most likely means entering a statement of disagreement with something in your record);
• tell you how to file a complaint about what you believe is an abuse of your privacy rights with the Office for Civil Rights (OCR) [17] of the Department of Health and Human Services (HHS); and
• tell you who to contact for more information about the provider or health plan’s privacy policies.

The HIPAA Privacy Rule also gives you a right to know who has accessed or received information from your PHR (called an “accounting of disclosures”). However, it is unclear how this works with PHRs since you would generally be the one accessing your own PHR, and anyone else who accesses it would need your permission. It has been suggested that providers who offer PHRs include a functionality that lets you view an access log.

Some additional protections you have with a HIPAA-covered PHR are not described in the notice of privacy practices. Recent updates to HIPAA require your provider or health plan to notify you if there is a breach of your medical records, 42 U.S.C. 17932(g) [18] Depending on the type of breach (negligent or intentional), there is a schedule of fines, ranging from $100 to $1.5 million.

OCR posts an up-to-date list [19] of all breaches affecting 500 or more individuals since 2009 is posted on its website. The PRC also has a searchable database of breaches [20] going back to 2005.

As this guide discusses below, the breach notification requirements and fines (but not the privacy and security regulations) also apply to commercial PHR vendors and others that offer products and services through a PHR vendor’s website. The Federal Trade Commission [21] has jurisdiction over data breaches involving non-HIPAA-regulated PHRs, based on its mandate to regulate unfair and deceptive trade practices.

HIPAA does not give you the individual right to sue whoever is responsible for the breach of your medical records. Only a state attorney general can bring a legal action.

b. When does California’s Confidentiality of Medical Information Act apply to PHRs?

California's Confidentiality of Medical Information Act (CMIA) applies to your individually identifiable medical information that either a covered entity (health care provider, health plan, or its contractors) has or that is derived from such information. It does not apply to information that you enter directly or that comes directly from a personal device or application that is not otherwise covered by regulations, such as health or fitness tracking hardware or software. See Cal. Civ. Code § 56.06(b) [22].

For businesses that are subject to it, the CMIA also imposes requirements for authorization to use any individually identifiable medical information they collect; the standard consumer “click to agree” terms of use is not sufficient. Unless the use or disclosure is for treatment, payment or health care operations—not likely in the case of a personal fitness tracker—it requires your specific and informed written authorization. A company that sells commercial PHRs, or devices or apps that collect medical information, and which has a business model based on selling or marketing that information, also needs your written authorization to use it. The way a business could side-step the need for authorization would be to use or disclose only aggregate information, which is theoretically unidentifiable.

c. Personal health records and the patient-physician privilege

State laws differ on the patient-physician privilege, but where they exist, the privilege protects confidential communications between you and your doctors and can prevent a doctor from having to testify about certain information that you share. However, it is possible to waive this privilege if you disclose the information to someone other than your doctor—that is, to a third party, like a PHR vendor. To waive the privilege in California, you must disclose information voluntarily, knowingly and with awareness of the consequences. See, for example, San Diego Trolley, Inc v. Superior Court [23].

d. What protections apply when medical privacy laws do not cover a personal health record?

If your employer offers a PHR, it typically won't be covered by HIPAA regulations. However, the PHR will be covered by HIPAA if it is part of an employer-sponsored health plan. An example of a PHR offered by employers is Dossia [24], which was created by a nonprofit consortium of major companies like AT&T, BP America, and Pitney Bowes, and is currently used by Walmart for its employees. Dossia also has a value-added wellness feature: it generates personalized health interventions by aggregating members’ PHR data and combining it with evidence-based health rules. An example would be notifying someone turning 50 about screening for colorectal cancer.

Just like most PHRs offered by employers, PHRs from commercial vendors, including mobile medical app vendors, will not be covered under HIPAA regulations. While some commercial PHRs may advertise themselves as “HIPAA-compliant,” the only privacy protections they must offer are those in their own privacy notices and practices, which they can change at any time. To give you an idea what to look for in a commercial PHR vendor’s privacy practices, the Office of the National Coordinator (ONC) at
the Department of Health and Human Services (HHS) has a model notice of privacy practices [25] for commercial PHR vendors. Note that it dates from 2011, and as of 2016 HHS is beginning the process of updating all of its privacy notices. [26]

Although HIPAA doesn’t cover this type of PHR and the information it contains, it still applies to your medical information before it can be transferred to the PHR. In other words, your health care provider needs your written authorization before disclosing your medical records directly to a PHR vendor. Alternatively, you may request your records from your health care provider and then provide those records to a PHR vendor.

Although a commercial PHR may not be covered by the HIPAA regulations it is still subject to breach notification requirements. A PHR vendor or a business that offers products and services through the vendor's website is liable for a breach of unsecured (unencrypted) health information, and must notify the affected individuals, the media if the breach involves 500 or more individuals, and the Federal Trade Commission (FTC). 42 U.S.C. § 17937 [27]

The FTC has helpful information [21] for vendors about who falls under this rule, what kind of incident requires a breach notification, and the specifics of notice (whom to notify, when, by what means, and with what information).

The FTC regulations do not give individuals the right to sue a PHR vendor for a breach of medical information, but California law does. And even if you cannot prove you were actually harmed by the breach, you are still entitled to nominal damages—damages that require no proof that you suffered actual harm—of $1000. Cal. Civ. Code § 56.36(b) [22]

The FTC forwards notices of PHR breaches that it receives from vendors to the HHS Office for Civil Rights (OCR). The FTC has enforcement authority over commercial PHRs and the OCR has enforcement authority over HIPAA-covered PHRs. OCR maintains a list [28] of all health-related data breaches that affect more than 500 individuals.

If you are considering using a commercial PHR, you should read its privacy notice and decide whether you are comfortable with the protections and rights the product offers. The following are some questions you should keep in mind when reading a PHR’s privacy notice.

- How will your information's security be safeguarded? Will it be encrypted when it is stored and transmitted? Does the vendor store your medical information in the cloud and how secure is that storage?
- What does the vendor say about how it may use or disclose your information? Does it mention disclosure of de-identified or aggregate data (a sure indication that it is selling the data)?
- What control do you have over access to the information in your PHR?
- Can you delete the PHR? What happens to the medical information that is in the PHR if you decide to cancel your account?

Also, a PHR vendor may, in some cases, share your health information with its contractors or other business partners. If that is the case, you’ll want to know whether these contractors or business partners will be limited in how they use or disclose the individual’s health information.

5. What should you look for to help you choose a commercial personal health record?

There are two documents you should read if you are trying to choose a commercial PHR from among several products, or are deciding if a PHR is for you at all. One is the vendor’s notice of privacy practices and the other is its privacy policy. A notice of privacy practices applies specifically to the PHR product and the information collected in it; a privacy policy explains the company’s overall privacy and security policies. You might want to beware of a PHR product whose notice of privacy practices and company privacy policy are difficult to find on its website, and to avoid any PHR product that does not provide one or both of those important items.

a. Notice of privacy practices

A PHR’s notice of privacy practices should really tell you everything you need to know about the product, including how much control the vendor allows you to have over your medical information. The Department of Health and Human Services has some very helpful information about how to evaluate this notice, based on its own model notice of privacy practices for PHR vendors [29] (now in the public comment phase of being revised). A Consumer Guide [30] that accompanies the notice thoroughly explains the important sections about what information the vendor says it will or will not release and what control you have over the information in your PHR, along with what security measures the vendor takes.

A notice of privacy practices should be clear about what information a PHR vendor will release, and in what form, either as personally identifiable medical information or statistical information that does not contain personal identifiers. At minimum, the
notice of privacy practices should include information about whether the vendor will release either personal or statistical information for the following purposes:

- marketing and advertising;
- medical and pharmaceutical research;
- reporting about company and customer activity (for example, customer-satisfaction reports for marketing purposes or reports to industry analysts or stockholders);
- to your insurer and/or employer (this would apply only to an employer- or insurer-sponsored PHR);
- developing software applications (that is, does the vendor share personal or statistical data with developers of improvements or add-on applications for the PHR?).

Next, the notice should tell you whether the PHR vendor has agreements with third parties that limit what the third parties may do with personal or statistical data the PHR vendor shares. Finally the vendor should tell you what happens to your data if you cancel or transfer your PHR. Does the vendor keep the data and continue sharing it according to the notice or destroy all the data that is in your PHR?

The notice should have a security section that assures you that the vendor has security measures in place that are reasonable and appropriate, or meet industry standards, or that are HIPAA compliant. Encryption would be a welcome security addition, although HIPAA doesn’t require it. It should tell you that the vendor will protect the information in your PHR from any unauthorized access, disclosure, or use. It should tell you that your PHR data is stored in the U.S., because if it is not, it will not be protected by any U.S. laws. And it should tell you if it keeps activity logs of who has accessed your PHR and when, and whether you have access to this information yourself.

b. Privacy policy

A web-based PHR vendor that collects personal information from California residents must have a privacy policy that tells you what personally identifiable information it collects and with whom it may share that information. Personally identifiable information would include both medical and demographic information, such as name, age, gender, address, phone number, email address, and credit card number. Cal. Bus. & Prof. Code §§ 22575–22579

With PHR vendors there may be confusion about whether the website privacy policy applies to information collected on the website or information that goes into the PHR. In some instances, it may apply to both, and cover medical and non-medical personally identifiable information.

6. Additional resources

California Office of the Attorney General, Privacy Enforcement and Protection Unit [31]: PHR fact sheet, Is a Personal Health Record Right for You? [32]

U.S. Department of Health and Human Services – Office of the National Coordinator (ONC)
Office of the National Coordinator for Health Information Technology [33]
Telephone: 202-690-7151
Fax: 202-690-6079
Email: onc.request@hhs.gov [34]


HHS – Office for Civil Rights (OCR)
Toll Free: 1-877-696-6775
To file a complaint [35] about what you believe is a privacy violation regarding your PHR.

Federal Trade Commission [36] If you have a complaint [37] about a PHR vendor that is not covered by HIPAA, you can contact the FTC at 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. To file a complaint with the FTC, this is the best place to begin: The FTC keeps a database of complaints in the Consumer Sentinel Network [38], which helps many civil and criminal law enforcement investigators with their research.

Food and Drug Administration (FDA) [39]
The FDA has issued a nonbinding guidance primarily for developers of mobile medical applications. It also distinguishes what is a regulated medical device from an unregulated mobile app: Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff [8]
AHIMA sponsors a website, MyPHR, with extensive tips and resources about PHRs for individuals with different medical information needs; i.e., seniors, parents, the chronically ill, caregivers and physicians. The site also offers a Quick Guide to Creating a PHR.

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
[6] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.06.&lawCode=CIV
[12] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.06.&lawCode=CIV
[22] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.36.&lawCode=CIV
[29] https://www.healthit.gov/policy-researchers-implementers/model-privacy-notice-mpn
[31] https://oag.ca.gov/privacy
[32] https://oag.ca.gov/privacy/facts/medical-privacy/health-record
[33] https://www.healthit.gov/
[34] mailto:onc.request@hhs.gov
[35] https://www.hhs.gov/hipaa/filing-a-complaint
[37] https://www.ftccomplaintassistant.gov/
[38] http://www.ftc.gov/sentinel/
[39] https://www.fda.gov/