Uploaded to the VFC Website

July 2014

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of "Frequently Asked Questions, please go to:

Veterans-For-Change

If Veterans don't help Veterans, who will?

Note: VFC is not liable for source information in this document, it is merely provided as a courtesy to our members & subscribers.

Fact Sheet 8:
Medical Records Privacy

Posted March 1993
Revised April 2013

[Also see our FAQ on medical privacy.]

1. Introduction

Many people consider information about their health to be highly sensitive, deserving of the strongest protection under the law. Long-standing laws in many states and the age-old tradition of doctor-patient privilege have been the mainstay of privacy protection for decades.

The federal Health Insurance Portability and Accountability Act (HIPAA) sets a national standard for privacy of health information. It was implemented in 2003. But HIPAA only applies to medical records maintained by health care providers, health plans, and health clearinghouses - and only if the facility conducts certain transactions electronically. A great deal of health-related information exists *outside* of health care facilities and the files of health plans, and thus beyond the reach of HIPAA. (PRC Fact Sheet 8a: HIPAA Basics)

The HHS "Omnibus Rule," issued on January 25, 2013, makes substantial modifications to the HIPAA privacy, security, and data breach rules, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009.

The extent of privacy protection given to your medical information often depends on where the records are located and the purpose for which the information was compiled. The laws that cover privacy of medical information vary by situation. And, confidentiality is likely to be lost in return for insurance coverage, an employment opportunity, your application for a government benefit, or an investigation of health and safety at your work site.

In short, you may have a false sense of security. That's because medical information that is collected outside a HIPAA environment may not afford you HIPAA's basic privacy rights to (1) access your medical records (2) request an amendment to your records and (3) request an accounting of disclosures. This guide provides information on medical records *not covered by the HIPAA Privacy Rule.*

2. What do my medical records contain?

Medical records are created when you receive treatment from a health professional such as a physician, nurse, dentist, chiropractor, or psychiatrist. Records may include your medical history, details about your lifestyle (such as smoking or involvement in high-risk sports), and family medical history.

In addition, your medical records contain laboratory test results, medications prescribed, and reports that indicate the results of operations and other medical procedures. Your records could also include the results of genetic testing used to predict your future health. And they might include information about your participation in research projects.

Information you provide on applications for disability, life or accidental insurance with private insurers or government programs can also become part of your medical file.

3. What medical information is not covered by HIPAA?

Medical information that is not covered by the federal privacy rule might be found in your financial records, your child's school records, and/or your employment files.

Financial records. The federal Gramm-Leach-Bliley Act (GLB) allows financial companies such as banks, brokerage houses, and insurance companies to operate as a single entity. GLB gives you the right to be notified about the information-sharing practices of financial institutions. And you must be given an opportunity to opt-out of third-party information sharing. But GLB does not keep information from being shared among affiliated companies.

Your credit card account and checking transactions are likely to include information about where you go for health care. Insurance applications and medical claims also contain health-related information. So it is possible for such medical information to be shared among affiliates of financial institutions. Such information is *not* protected by HIPAA.

Some financial companies promise extra protection for medical information. And insurance companies may be prohibited from giving information to an affiliated bank by state insurance laws. It pays to examine the privacy notices of financial institutions carefully. (Read PRC Fact Sheet 24: Protecting Financial Privacy.)

In addition, the Fair Credit Reporting Act (FCRA) limits the way financial companies can use medical information when you apply for credit. For example, if you apply for a car loan, the lender can consider debts for unpaid medical bills just like any other debt. However, the lender cannot ask about your medical condition and must treat medical bills like any other debt in deciding whether to give you a loan. Another section of this law now says that credit bureaus cannot report the name, address or telephone number of any medical creditor, unless the information is reported in code.

For more on your medical information, lenders and the credit bureaus, see PRCFact Sheet 6b: FACTA, The Fair and Accurate Credit Transactions Act.

Education records maintained by your child's school contain vaccination histories, information about physical examination for sports, counseling for behavioral problems, and records of visits to the school nurse. Privacy of education records is under the control of the U.S. Department of Education and the Family Educational Rights and Privacy Act (FERPA). These records are not covered by HIPAA.

For more information about FERPA, visit the Department of Education's website on FERPA.

Also see guidance on education records and HIPAA issued jointly by the Department of Education and the Department of Health and Human Services.

Employment records and medical information may be mingled in situations not covered by HIPAA. Your employer may be covered by the Occupational Safety and Health Act (OSHA). If so, you have the right to access your medical records gathered for your employer's OSHA responsibilities. (Seehttp://www.osha.gov/Publications/pub3110text.html).

In addition, the federal Family and Medical Leave Act (FMLA) gives most workers the right to 12 weeks of unpaid leave a year for personal and family health. If FMLA leave is because of a serious illness, your employer may request a doctor's certification of the illness. But the employer cannot make you produce medical records. See the U.S. Department of Labor website for more information on FMLA.

Employers, in an effort to control rising healthcare costs, now offer a variety of health and fitness programs. Many programs, often called Employee Health Programs or EHPs, are offered by outside contractors that service multiple employers.

EHPs may be as simple as a lunchtime exercise class or include a highly-structured weight loss plan with personal trainers, individualized diets, exercise plans and close monitoring of weight, blood pressure, or body mass index. Employees, in some case, may also receive counseling for personal and family problems or substance abuse through programs established by their employer. Such programs are generally not covered by HIPAA. As such, there is no universal privacy standard that applies to all programs.

If your employer is self-insured for employees' medical benefits, its handling of insurance claims and other health-related information is covered by HIPAA. In this capacity, the employer would be considered a "hybrid" entity. For more information on HIPAA involving employer group health plans and self-insurance situations, read PRC Fact Sheet 8a: HIPAA Basics.

4. Who has access to your medical records?

Your medical information is shared by a wide range of people both in and out of the health care industry. Generally, access to your records is obtained when you agree to let others see them. In reality, you may have no choice but to agree to the sharing of your health information if you want to obtain care and qualify for insurance.

A. Insurance companies usually require you to release your records before they will issue a policy or make payment under an existing policy. This is especially true if you apply for individual health insurance as opposed to a group health plan available through your employer.

Insurance companies are considered financial institutions under the federal GLB law. Like banks and brokerage houses, they must provide you a notice of how they gather and use your customer information. You may have the right to opt-out of sharing some information with other companies.

To learn more about the insurance privacy laws in your state, visit your state's Department of Insurance website. Find your state's Department of Insurance by visiting the National Association of Insurance Commissioners website. Medical information gathered by an insurance company may also be shared with others through the Medical Information Bureau (see below).

B. Government agencies may request your medical records to verify claims made through Medicare, MediCal, Social Security Disability, and Workers Compensation.

C. The **Medical Information Bureau** (MIB Group, Inc.) is a central database of medical information shared by insurance companies. Approximately 15 million Americans and Canadians are on file in the MIB's computers. About 600 insurance firms use the services of the MIB primarily to obtain information about life insurance and individual health insurance policy applicants.When you apply for life or health insurance as an *individual*, you are likely to be asked to provide information about your health.

Sometimes you are required to be examined by a doctor and/or to have your blood and urine tested. If you have medical conditions that insurance companies consider significant, the insurance company will report that information to the MIB.The information contained in a typical MIB record is limited to codes for specific medical conditions and lifestyle choices. Examples include codes to indicate high blood pressure, asthma, diabetes, or depression. A code can signify participation in high-risk sports such as skydiving. A file would also include a code to indicate that the individual smokes cigarettes. The MIB uses 230 such codes.It's important to remember the following about the MIB:

- The MIB is subject to HIPAA as a business associate of its member health insurance companies. As a business associate of HIPAA "covered entity" insurance companies, MIB must comply with the data security standards adopted by the Health Information Technology for Economic and Clinical Health Act (HITECH), which was effective in February of 2010.
- MIB files do *not* include the totality of one's medical records as held by your health care provider. Rather it consists of codes signifying certain health conditions.
- A decision on whether to insure you is not supposed to be based solely on the MIB report.
- The MIB is also a consumer reporting agency subject to the federal Fair Credit Reporting Act (FCRA). If you are denied insurance based on an MIB report, you are entitled to certain rights under the FCRA, including the ability to obtain a free report and the right to have erroneous information corrected. See the Federal Trade Commission's website on insurance decisions.

The MIB does not have a file on everyone. But if you have an MIB file, you will want to be sure it is correct. You can obtain a copy for free once a year by calling (866) 692-6901. You may also order your file disclosure through MIB's website,www.mib.com/request_your_record.html A written request may be sent to MIB Disclosure Office, 50 Braintree Hill Part, Suite 400, Braintree, MA 02184.

D. IntelliScript and MedPoint are databases that report prescription drug purchase histories to insurance companies. Like the MIB reports, IntelliScript and MedPoint reports are used primarily when consumers are seeking private health, life or disability insurance. Prescription drug databases can go back as far as five years, detailing drugs used as well as dosage and refills.

With a history of prescription drugs in hand, insurers may make assumptions about medical conditions and assess the risk of writing an insurance policy. Information in an IntelliScript or MedPoint report may prompt an insurer to deny coverage for certain conditions, increase insurance premiums, or deny coverage altogether. Such adverse

actions by insurance companies trigger a sequence of consumer rights under the Fair Credit Reporting Act (FCRA).

Until recently, use of prescription drug databases was unknown to consumers. Insurers' use of these databases first came to light in 2007 when the Federal Trade Commission (FTC) sued Milliman, the owner of the IntelliScript database, and Ingenix, Inc., owner of the MedPoint database.

The FTC claimed that the companies are consumer reporting agencies subject to the FCRA. Both cases were settled without the data brokers paying a monetary penalty, but Milliman and Ingenix agreed to follow the FCRA. This means, among other things, that consumers who apply for private insurance and are turned down because of something in an IntelliScript or MedPoint report are entitled to a copy of the report from their insurance company and an opportunity to dispute the accuracy of information in the report.

Individuals who have applied for individual health, life or disability insurance may also request a copy of any prescription report directly from MedPoint or IntelliScript. Reports are available once a year whether or not there has been an adverse decision by an insurance company.

You can request a copy of your MedPoint report by calling (888) 206-0335 or writing to: MedPoint Compliance, Ingenix, Inc., 2525 Lake Park Blvd, West Valley City Utah 84120.

IntelliScript reports are available by calling the toll-free request line at (877) 211-4816. Consumers will have to provide their full name, date of birth, last four digits of their Social Security number and current zip code. Milliman will provide a copy of any information the company has on an individual as well as the names of insurance companies that have requested a prescription history. The Milliman webpage "How does it work?" includes information about the product as well as additional contact information.

E. Employers usually obtain medical information about their employees by asking employees to authorize disclosure of medical records. This can occur in several ways not covered by HIPAA. Unfortunately, the laws in only a few states require employers to establish procedures to keep employee medical records confidential. (For example, California Civil Code §56.)

A potential employer may ask for medical information as part of an employment background check, with limitations as explained below. To learn more on employment background checks and an employer's obligations under the FCRA, read PRC Fact Sheet 16: Employment Background Checks, and the FTC's website on background checks.

According to the federal Americans with Disabilities Act in workplaces with more than 15 employees (ADA text, 42 USC §12101 et seq.)

- Employers may not ask job applicants about medical information or require a physical examination prior to offering employment. After employment is offered, an employer can only ask for a medical examination if it is required of all employees holding similar jobs.
- If you are turned down for work based on the results of a medical examination, the employer must prove that it is physically impossible for you to do the work required.

Report violations of the ADA to the U.S. Equal Employment Opportunity Commission (EEOC). Phone: (800) 669-4000. Web: www.eeoc.gov.

For more on health information in the workplace, see the Department of Health and Human Services webpage on Employers and Health Information in the Workplace.

F. Your medical records may be **subpoenaed for court cases**. If you are involved in litigation, an administrative hearing, or a worker's compensation hearing and your medical condition is an issue, the *relevant* parts of your medical record may be copied and introduced in court. Whether or not some or all of your medical information is deemed "relevant" may depend on the judge or skill of the attorneys involved.

In addition, law enforcement officials may receive protected health information in other situations such as an instance of abuse, a death, a gunshot or stabbing. For more on circumstances that allow law enforcement to have access to medical information, seehttp://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/index.html.

G. Other disclosures of medical information occur when medical institutions such as hospitals or individual physicians are evaluated for quality of service. This evaluation is required for most hospitals to receive their licenses. Your identity may or may not be disclosed when medical practices are evaluated. Evaluations for accreditation are called "health care operations" under HIPAA. Consent to use your information for these purposes is usually not required.

Occasionally your medical information is used for health research and may be disclosed to public health agencies like the Centers for Disease Control. Specific names are usually not given to researchers. Their use of patient information is covered by HIPAA. (http://www.hhs.gov/ocr/privacy/hipaa/faq/research_disclosures/index.html and PRC Fact Sheet 8a: HIPAA Basics)

H. Medical information may be passed on to **direct marketers** when you participate in informal health screenings. Tests for cholesterol levels, blood pressure, weight and physical fitness are examples of free or low-cost screenings offered to the public. Screenings are often conducted at pharmacies, health fairs, shopping malls, or other nonmedical settings. The information collected may end up in the data banks of businesses which have products to sell related to the test.

I. A tremendous amount of health-related information is found on the **Internet**. Many discussion forums are available for individuals to share information on specific diseases and health conditions. Websites dispense a wide variety of information. There is no guarantee that information you disclose in any of these forums is confidential. Always review the privacy policy of any website you visit.

5. How can I protect the privacy of my medical records?

The federal law on medical privacy, HIPAA, went into effect in 2003. For the first time, federal law established standards for patient privacy in all 50 states, including the right of patients to access to their own records. The stronger laws already in effect in the states were not weakened. Although HIPAA provides some protection, it is not the final answer to medical records privacy. Here are some strategies to limit others' access to your medical records:

A. Discuss your confidentiality concerns with your doctor. If you want a specific condition to be held in confidence by your personal physician, bring a**written request** to the appointment that revokes your consent to release medical information to the insurance company and/or to your employer for that visit. You must also pay for the visit yourself rather than obtain reimbursement from the insurance company.

To be especially certain of confidentiality, you may need to see a different physician altogether and **pay the bill yourself**, forgoing reimbursement from the insurance company. Realize that under HIPAA, your attempts to restrict the sharing of specific records can be denied by the health care provider.

B. Ask your health care provider to use caution when **photocopying** portions of your medical records for others. Sometimes more of your medical records are copied than is necessary, for example, when requested by the insurance company or another health care provider.

C. Find out if your health care provider has a policy on the use of **cordless and cellular phones** and **fax machines** when discussing and transmitting medical information. Wireless telephones are not as private as standard "wireline" telephones. Because they transmit by radio wave, phone conversations can be overheard on various electronic devices. Digital systems are more secure. (See PRC Fact Sheet 2: Wireless Communications)

Fax machines offer far less privacy than the mail. Frequently many people in an office have access to fax transmissions. Staff members at all levels of the organization should take precautions to preserve confidentiality when sending and receiving medical documents by fax machine. (See PRC Fact Sheet 12: Checklist of Responsible Information Handling Practices)

Your medical information is not confined to health care institutions. Here are some additional situations where you must be careful to protect your privacy.

D. If your records are **subpoenaed** for a legal proceeding, they become a public record. Ask the court to allow only a specific portion of your medical record to be seen, or better yet, not to be open at all. A judge will decide what parts, if any, of your medical record should be considered private. After the case is decided, you can also ask the judge to "seal" the court records containing your medical information.

E. If **your employer** is self-insured, the human resources department is likely to have information about any health-related claims that you file. If you are concerned about the privacy protection policies and practices of your employer, talk to the appropriate administrator. You should consider following up with a letter to the head of the department that handles health-related information. Diplomatically stress your desire for all of your health information to be handled with the utmost confidentiality. Keep a copy for yourself, filed at home.

F. Think twice before filling out **marketing-related questionnaires**. They commonly contain sections that ask for a great deal of family health information. The loss of your medical privacy is a high price to pay in exchange for a few free coupons or a chance to win a contest. For more information, read the PRC' s 2001 testimony to the Federal Trade Commission.

G. Before participating in **health screenings** offered in shopping malls and other public places, find out what uses will be made of the medical information that is collected. If you are not given the opportunity to say "no" to the sharing of your medical information with others, don't participate.

H. Use caution when visiting **health-related websites** and when participating in online discussion groups.

- Carefully read the privacy policies and terms of services of medical websites. Do not fill out registration forms unless you are satisfied with the web operator's privacy policy.
- Use a pseudonym when participating in chat rooms and online forums.
- Before sharing personal information with a health website, find out if it participates in a web seal program such as TRUSTe, URAC Health Web Site Accreditation, HON (Health on the Net) and BBBOnline.

- Remember, companies can change their privacy policies at any time. And if the company goes bankrupt, its data base of user information could be sold to the highest bidder.

I. Establish your own history of treatment. If you decide to change physicians or health care organizations, it is a good idea to obtain copies of your medical records. Physicians may retire, move out of state or merge practices with other physicians. Health care facilities may merge with another facility or even go out of business following bankruptcy. Get copies of medical records while you can. Don't count on your ability to get your records years after treatment. If your doctor or health care provider goes out of business, be sure to find out where they intend to store the medical records of their patients.

Although HIPAA does not require that medical records be kept for a set time, federal rules or states may have such laws. To learn more about medical records and retention periods, see the American Health Information Management Association (AHIMA) guidelines with links to federal requirements:http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049252.hcsp?dDocName=bok1_049252

J. If your employer offers an employee health or wellness program, an **EHP**, ask about any established privacy policy. You want to know whether your progress reports will be maintained by an outside consultant or made a part of your permanent personnel file.

K. Be on guard against employers or health insurers that ask for your permission or require you to submit to genetic testing. A 2008 federal law, the Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and most health insurance plans from denying you employment or health benefits based on genetic information. In addition, on October 9, 2009, the U.S. Department of Health and Human Services, joined by the U.S. Department of Labor and U.S. Department of the Treasury, issued interim final rules implementing GINA's nondiscrimination provisions. Among other things, HHS has determined that genetic information, like other health-related information, is subject to the privacy protections of HIPAA.

The interim final regulation can be found here:www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/ginaifr.pdf

In November 2010, the EEOC issued a final regulation to implement GINA.https://www.federalregister.gov/articles/2010/11/09/2010-28011/regulations-under-the-genetic-information-nondiscrimination-act-of-2008

In addition, the non-profit organization Council for Responsible Genetics (CRG) has extensive information available on privacy and genetics. CRG's website also includes tips on how to protect your genetic privacy. www.councilforresponsiblegenetics.org/geneticprivacy/tips.html

6. How do I get access to my own medical records?

HIPAA requires health care providers, health plans, and health care clearinghouse to allow you access to your medical records. Notices you receive from providers and plans must include information about how you can obtain copies of your medical records.

HIPAA allows health care providers, health plans, and health care clearinghouses to impose reasonable, cost-based fees to obtain copies of your medical records. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive

a summary or explanation of his or her protected health information, the entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information.http://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_access_medical_records/353.html.

In addition to HIPAA, about half the states have laws that allow patients or their designated representatives to access medical records. The HHS publication on Personal Representatives discusses access by personal representatives.

If you receive care in a federal medical facility, you have a right to obtain your records under the federal Privacy Act of 1974 (5 USC sec. 552a)

We advise that you make your request in writing. See the PRC Sample Letter to Request Medical Records. If you are denied access, you can file a complaint with the U.S. Department of Health and Human Service's Office of Civil Rights. (Contact information is provided at the end of this guide). Your state's medical privacy law might also enable you to file a complaint with state regulators.

7. How can I learn more about the federal privacy rule, HIPAA?

The 1996 federal Health Insurance Portability and Accountability Act (HIPAA) mandated the development of federal regulations to be adopted by the U.S. Department of Health and Human Services (DHHS). The regulations were confirmed by the Secretary of DHHS in April 2001, and were effective April 14, 2003. The implementation date for small health plans was April 14, 2004.

In addition to the PRC's Fact Sheet 8a: HIPAA Basics, and the DHHS Office of Civil Rights website has extensive information on HIPAA. HIPAA changes required by HITECH can be found in the HHS "Omnibus Rule" issued on January 25, 2013. For a summary of significant changes made by the Omnibus Rule, see the American Health Information Management Association's March 25, 2013 release.

A hotly debated provision of HIPAA was the creation of a national health care identification number for everyone. Due to strong opposition by the public and members of Congress, that idea was tabled.

In the years since HIPAA took effect, one of the most widely heard criticism is that the rules were not effectively enforced. Major revisions adopted in February 2009 as part of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), also known as the Stimulus Law, call for enhanced enforcement and stiffer penalties for violations. For more on how the Stimulus Law related to healthcare and enforcement of privacy rights, see PRC Fact Sheet 8a: HIPAA Basics.

8. Do any state laws protect the privacy of my medical records?

HIPAA sets the "floor" on privacy rights. That means states are free to adopt more stringent medical privacy laws, but states cannot pass any law that takes away your HIPAA rights.

It is quite possible your state has adopted laws that give you greater privacy rights than those you have under HIPAA. For example, a California law gives you the right to sue for privacy violations. The new law also covers many health care services generally not covered by HIPAA, including:

- Home health agencies.
- Hospices.
- Mobile health care units.

- Acute psychiatric hospitals.
- Intermediate care facilities.

For more on medical privacy rights in California, see PRC Fact Sheet 8a: HIPAA Basics, and the website for the California Office of Health Information Integrity (CALOHI), www.ohii.ca.gov/calohi/

Also see PRC's microsite dedicated solely to medical privacy in California,www.privacyrights.org/california-medical-privacy and the California Attorney General's Privacy Enforcement and Protection Unit, https://oag.ca.gov/privacy

For information on medical privacy rights in other states, see Georgetown University Center on Medical Record Rights and Privacy.

9. Electronic health records: What are the benefits and dangers for consumers

In January 2005 the Bush Administration called for the creation of a nationwide network of electronic health records (EHR) within 10 years.

There are both benefits and very real pitfalls to such a grandiose scheme. Certainly, access to electronic records would have greatly assisted emergency health teams in the aftermath of Hurricane Katrina in August 2005. And most individuals can easily envision the benefits to hospital emergency rooms when assisting unconscious patients. But the challenges regarding security and confidentiality are profound.

To become better informed about this national initiative, visit these websites:

- U.S. Dept. of Health & Human Services (DHHS) information technology page,http://www.healthit.gov/
- The DHHS's creation of the American Health Information Community, AHIC:http://archive.healthit.hhs.gov

The need for EHRs as part of a plan to overhaul the nation's health care systems was one of the few points on which the in 2008 presidential candidates could agree. In January 2009, President Obama signed the American Recovery and Reinvestment Act of 2009, Public Law No: 111-5, also known as the Stimulus Law, which allocates 19 billion dollars for electronic health records by the year 2014.

Title XIII of this sweeping legislation, known as the Health Information Technology for Economic Health Act added new provisions for HIPAA's privacy, security and enforcement rules.

To learn more about the 2009 Stimulus Law and HITECH, see PRC Fact Sheet 8a: HIPAA Basics.

Electronic health records, EHRs, refers to a government-promoted technological system that allows health care providers to consolidate, store, retrieve and share medical information about an individual's entire medical history. EHRs, with the goal of eventually making paper records obsolete, are endorsed as a way to save money and reduce medical errors.

Personal Health Records (PHRs). Various commercial systems for storing medical records have also emerged in recent years. Such systems, operated by Internet vendors are called personal health records or PHRs, and allow consumers to create their own health history.

One example of PHR is the Microsoft HeathVault website. HealthVault is a service for storing, managing, and accessing a patient's medical information. It operates as an online encrypted service. The service offers a

voluntary opportunity for medical records to be collected by aggregating information from various sources including health-care providers, insurance companies, and compatible medical devices (such as blood pressure monitoring devices).

These types of aggregated electronic health records pose a number of concerns:

- The custodian of the records may not necessarily be a "covered entity" under the HIPAA privacy rule. HIPAA only applies to health care providers, health plans, and health care clearinghouses. Therefore, it is possible that consumers may not have any privacy rights under the HIPAA law if they utilize a service that electronically aggregates medical records.
- The website operator could become subject to judicial process and can be served with a subpoena for your personal medical records. This greatly facilitates the ability of both government entities and civil litigants to go on "fishing expeditions" for your medical records.
- The website's privacy policy can be changed at any time. This could, for example, subject consumers to targeted advertising based upon their medical conditions.

For more on PHRs, see PRC Alert: Online Personal Health Records: Are They Healthy for Your Privacy, April 21, 2009.

Also see the World Privacy Forum's Personal Health Records Page. And see, the California Attorney General's Privacy and Enforcement and Protection Unit's publication, Is a Personal Health Record Right for You?

10. Resources for additional information

HIPAA

U.S. Department of Health and Human Services
Office of Civil Rights
200 Independence Avenue, S.W.
Washington, D.C., 20201
Phone: (866) 627-7748
Web: www.hhs.gov

Read PRC Fact Sheet 8a, "HIPAA Basics: Medical Privacy in the Electronic Age,"www.privacyrights.org/fs/fs8a-hipaa.htm

Visit PRC's California medical privacy microsite, www.privacyrights.org/california-medical-privacy

Contact the **U.S. Department of Labor** regarding privacy of medical information in the workplace, including your employer's health and safety files and family-leave records.

U.S. Department of Labor
200 Constitution Ave., NW
Washington, DC 20210
Phone: (866) 4USA-DOL (866-487-2365)
Web: www.dol.gov
Web link to 50 states' Labor services:www.dol.gov/dol/location.htm

Contact the **Federal Trade Commission** to learn about health information collected for:

- Employment background checks,www.ftc.gov/bcp/edu/pubs/business/credit/bus08.shtm
- Applications for insurance coverage,www.ftc.gov/bcp/edu/pubs/business/credit/bus07.shtm

For help with the federal **Americans with Disabilities Act**, call the nearest Technical Assistance Center.

- Phone: (800) 949-4232
- Web: www.adata.org, and for the western states, www.adapacific.org.

State medical boards:

- In California, for health privacy-related disputes regarding doctors, contact the Medical Board of California at (800) 633-2322. Web: www.medbd.ca.gov
- Complaints about California HMOs can be filed with the Department of Managed Health Care. Phone: (888) 466-2219. Web: www.hmohelp.ca.gov.
- To link to medical boards in the 50 states, visit the American Medical Association website: www.ama-assn.org/ama/pub/category/2645.html

Other Resources

Georgetown University's Center on Medical Records Rights and Privacyoffers state-specific guides on accessing your medical records,http://hpi.georgetown.edu/privacy/records.html.

The **World Privacy Forum** examines the relationship between privacy, security, confidentiality and electronic health records. www.worldprivacyforum.org

California Attorney General's Privacy Enforcement and Protection Unit,https://oag.ca.gov/privacy/facts/medical-privacy/health-record

Electronic Frontier Foundation's Medical Privacy page,https://www.eff.org/issues/medical-privacy