Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Introduction to Health and Medical Information Privacy [1]

Posted Aug 01 2014
Revised Aug 01 2014

1. Introduction

The facts of a particular situation will dictate the extent to which medical information receives privacy protection. For example, it is important to consider who has the information and why it was created. In addition, individuals trade confidentiality daily in return for things such as insurance coverage, employment opportunities, government benefits, or worksite health and safety investigations.

The federal Health Insurance Portability and Accountability Act (HIPAA) sets a national standard for health information privacy. But HIPAA only applies in certain situations [2], and a great deal of health-related information exists beyond its reach.

2. What types of health and medical information exist?

Health professionals create medical records when they treat patients. Records may include medical history, lifestyle details (such as smoking or involvement in high-risk sports), and family medical history. They may also include laboratory test results, medications prescribed, surgery results, genetic testing results, and research participation.

Health and medical information is also collected from individuals when they apply for disability, life, or accident insurance through private insurers or government programs.

In addition, individuals often generate health and medical-related information themselves. They search for illnesses and medical products online, they join support groups, they use mobile applications to monitor their health and fitness, and the list goes on.

3. Who may have access to health and medical information?

A wide range of people, companies, and government agencies both within and outside of the health care industry can have a surprising amount of access to health and medical information that individuals might otherwise assume is private. Below are some very general examples.

a. HIPAA covered entities and their business associates

Healthcare providers, health plans, and healthcare clearinghouses (collectively called "covered entities [3]") have access to medical records and health information but are also required to comply with HIPAA. Covered entities' "business associates [4]" must also comply with HIPAA. For more information about protected health information covered under HIPAA, see PRC's consumer guide [5].

b. Insurance companies

Insurance companies usually require individuals to release records before they will issue a policy or make a payment under an existing policy. This is especially true for individual health insurance as opposed to a group health plan available through an employer. Many types of insurance companies must comply with HIPAA [6] as health plans, but certain types of insurers are not required to comply with HIPAA [7].

Like banks and brokerage houses, insurance companies are subject to a federal law called the Gramm-Leach-Bliley Act [8] (GLB) and must provide individuals with a privacy notice stating how they gather and use certain customer information. In some situations they are required to provide customers a right to opt-out of sharing some information with other companies.

Regardless of whether there is an applicable federal law, it is important to also research state laws. To find the applicable state's insurance department, visit the. National Association of Insurance Commissioners website [9].

c. The Medical Information Bureau

The Medical Information Bureau (MIB Group, Inc [10].) is a database of medical information shared by life and health insurance companies. Insurance companies use the MIB primarily to obtain information about life insurance and individual health insurance policy applicants for the purposes of assessing risk and eligibility.

When *individuals* apply for insurance policies themselves, they will likely be asked to provide health information or submit to testing such as a blood or urine test. If the applicant has medical conditions that insurance companies consider significant, the insurance company will report that information to the MIB.

The information 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 hundreds of such codes.

It's important to remember the following about the MIB:

- The MIB is subject to HIPAA as a business associate [4] of its member health insurance companies.
- MIB files do *not* include the totality of one's medical records as held by a health care provider. Rather it consists of codes signifying certain health conditions.
- A decision on whether to insure 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 a person is denied insurance based on an MIB report, he or she is 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 [11].

The MIB does not have a file on everyone, and won't have information on someone who has not applied for *individually underwritten* life or health insurance in the last seven years. However, people who believe they have an MIB file will want to be sure it is correct.

Individuals can obtain a copy for free once a year by calling (866) 692-6901 or ordering it through MIB's website [12].

Individuals may submit written requests to:

MIB Disclosure Office
50 Braintree Hill Part, Suite 400
Braintree, MA 02184

d. Prescription drug database companies

Two companies, Milliman (IntelliScript [13]) and Ingenix (MedPoint [14]) buy prescription information from pharmacy benefit managers [15] (PBMs) and compile it into reports. They sell these prescription drug purchase history reports to insurance companies.

Prescription drug reports cover prescriptions over a five-year period, and include dosages, dates, refills, and prescribing doctors. Insurers typically use prescription drug history reports to verify information, determine risk, and set premiums when individuals apply for private health, life, or disability insurance.

In 2007, the Federal Trade Commission (FTC) issued a consent order [16] stating that Ingenix and Milliman are consumer reporting agencies (CRAs) subject to the Fair Credit Reporting Act (FCRA). Prescription reporting companies are CRAs because they compile and analyze consumer information (prescriptions) and furnish it to insurers to use in determining individuals' eligibility for insurance.

The FTC's action settled claims that the companies violated the consumer-reporting law by failing to notify insurers of their responsibilities under the FCRA. These responsibilities include, among other things, notifying individuals who are denied insurance because of their prescription reports and providing them with a means to request a copy of the report and have any errors corrected. For more information on the FCRA, see PRC's consumer guides on Credit & Credit Reports [17].

Individuals who have applied for individual health, life or disability insurance may request a copy of any prescription report directly from MedPoint or IntelliScript and also request that the companies correct any inaccurate information.

Individuals can request a 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 (877) 211-4816. Individuals 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 website [18] contains information about the product as well as additional contact information.

e. Financial institutions

Financial transactions are likely to reveal information about where an individual goes for healthcare. This kind of information is not covered under HIPAA. However, the federal Gramm-Leach-Bliley Act [8] (GLB) requires financial institutions to notify individuals of information-sharing practices and provide an opt out for certain third party sharing. Regardless, some financial companies may offer extra protection for medical information so it is importnant to read financial institutions' privacy notices and ask questions. For more information, see PRC Fact Sheet 24a: *Financial Privacy: How to Read Your "Opt-Out" Notices [19].*

f. Government agencies

Government agencies on all levels (local, state, and federal) may request or receive certain types of health or medical information. For example, government agencies may request medical records or information to verify claims a person makes through Medicare, MediCal, Social Security Disability, and Workers Compensation. For more information on government access to medical information (and additional examples), see PRC's consumer guide *Health Privacy outside the Healthcare Environment: Health Records on the Job, Available to the Government, and in Credit Reports* [20].

g. Educational institutions

Educational institutions may have records that contain vaccination histories, information about physical examination for sports, counseling for behavioral problems, and records of visits to the school nurse among other things. Privacy of education records is under the control of the U.S. Department of Education and the Family Educational Rights and Privacy Act (FERPA). HIPAA does not cover education records. For more information about FERPA, visit the Department of Education's website on FERPA [21].

h. The court system and law enforcement

When a person is involved in litigation, an administrative hearing, or a worker's compensation hearing and his or her medical condition is an issue, the *relevant* parts of a medical record may be introduced in court.

In addition, law enforcement officials may receive health information [22] in situations such as an instance of abuse, a death, a gunshot or stabbing.

If records are for a legal proceeding, they become a part of public record. However an individual can ask the court to allow only a specific portion of a medical record to be seen (by redacting certain information), or better yet, not to be open at all (by sealing the record). Individuals should consult legal counsel for more information.

i. Employers

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. Depending on state law, employers may have to establish procedures to keep employee medical records confidential. For information on California-specific laws, see PRC's California Medical Privacy Guides [23]. For more information on health privacy generally as it applies to employment, see PRC's consumer guide *Health Privacy outside the Healthcare Environment: Health Records on the Job, Available to the Government, and in Credit Reports* [20].

Tip: When an employer offers an employee health or wellness program, employees should ask about any established privacy policy. It is particularly important to know whether progress reports will be maintained by an outside consultant or made a part of a permanent personnel file.

j. Marketers and data brokers

Health- and medical-related information may be passed on to marketers and data brokers when individuals participate in informal health screenings or otherwise voluntarily release information [24] in a situation that doesn't fall under HIPAA or stronger state law. The World Privacy Forum's report, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* [25], explains potential consumer harms in a broader context and addresses health information privacy.

Tips: Think twice before filling out marketing-related questionnaires. They commonly contain sections that ask for a great deal of family health information. Losing control over health or medical information is a high price to pay in exchange for a few free coupons or a chance to win a contest.

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. Make sure the screeners give individuals the opportunity to opt out of or restrict sharing the information.

k. Websites and mobile applications

A tremendous amount of health-related information is available on the Internet. Many sites and discussion forums are available for individuals to share information on specific diseases and health conditions. Websites dispense a wide variety of information, but they also collect a wide variety of information. There is no guarantee of confidentiality when a site isn't subject to medical privacy laws (and most aren't).

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

- Carefully read the privacy policies and terms of service of medical websites. Individuals should not fill out registration forms unless they are satisfied with the web operator's privacy policy.
- Use a pseudonym when participating in chat rooms and online forums.
- Remember, companies can change their privacy policies at any time.

Mobile health and fitness applications (apps) are also widely available to consumers and generate a lot of information that individuals might consider sensitive. Just as is the case with websites and services, it is important to read the app's privacy policy. For more information, see PRC's consumer guide *Mobile Health and Fitness Apps: What are the Privacy Risks?* [26]

Personal Health Records (PHRs). PHRs allow consumers to store, manage, and share their health information. Individuals manage their own PHRs which is what distinguishes them from electronic health records (EHR) that a health care provider controls and populates. Various companies offer PHRs, and features vary. However many PHRs offer individuals the ability to store and transmit medical history information, prescription information, test results and imaging, drug alerts, immunization records, and treatment plans.

These types of aggregated electronic health records pose a number of privacy risks, here are a few:

- HIPAA and/or state health privacy laws may not apply to a PHR.
- The website operator could be asked to turn over customer records as part of a legal proceeding.
- Website privacy policies are subject to change.

For more information about PHRs, the California Attorney General's Privacy and Enforcement and Protection Unit has a publication title *Is a Personal Health Record Right for You?* [27] The Office of the National Coordinator (ONC) within the Department of Health and Human Services (HHS) has a model notice of privacy practices [28] for commercial PHR vendors. In addition, the World Privacy Forum's Personal Health Records Page [29] contains helpful information.

I. Anyone else to whom an individual reveals the information

It is important for individuals to understand HIPAA's limits [2]. The best policy is ask questions and do a little research before revealing health or medical information. There are many instances in which people create or release health or medical information and there are no applicable privacy laws. In these cases, it is best to look for and understand any relevant privacy policies the person or company has agreed to follow.

4. Resources

U.S. Department of Health and Human Services [30]
Office of Civil Rights
200 Independence Avenue, SW
Washington, D.C., 20201
Phone: (866) 627-7748

Privacy Rights Clearinghouse, Medical Privacy page [1].

Contact the **U.S. Department of Labor** [31] regarding privacy of medical information in the workplace, including employer health and safety files and family-leave records.

U.S. Department of Labor
200 Constitution Avenue, NW
Washington, DC 20210
Phone: (866) 4USA-DOL (866-487-2365)
[32]Link to 50 states' Labor services:www.dol.gov/dol/location.htm [33]

Contact the **Federal Trade Commission** or see the FTC website to learn about health information collected for employment background checks [34] and applications for insurance coverage.

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

- Phone: (800) 949-4232
- Web: www.adata.org [35], and for the western states, www.adapacific.org [36]

State medical boards:

- In California, for health privacy-related disputes regarding doctors, contact the Medical Board of California [37] at (800) 633-2322.
- Complaints about California HMOs can be filed with the Department of Managed Health Care [38]. Phone: (888) 466-2219.
- To find medical boards in all 50 states, visit the American Medical Association website [39].

Other Resources

The **World Privacy Forum** [40] examines the relationship between privacy, security, confidentiality and electronic health records.

California Attorney General's Privacy Enforcement and Protection Unit [27].

Electronic Frontier Foundation's Medical Privacy page [41].

Source URL (modified on November 30, 2016): https://www.privacyrights.org/consumer-guides/introduction-health-and-medical-information-privacy

Links
[1] https://www.privacyrights.org/consumer-guides/introduction-health-and-medical-information-privacy
[2] https://www.privacyrights.org/content/health-privacy-hipaa-basics

[3] https://www.privacyrights.org/content/health-privacy-hipaa-basics#covered%20entities
[4] https://www.privacyrights.org/content/health-privacy-hipaa-basics#business%20associate
[5] https://www.privacyrights.org/consumer-guides/health-privacy-hipaa-basics
[6] https://www.privacyrights.org/content/health-privacy-hipaa-basics#who%20must%20comply
[7] https://www.privacyrights.org/content/health-privacy-hipaa-basics#not%20required%20to%20comply%20HIPAA
[8] http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act
[9] http://www.naic.org/state_web_map.htm
[10] http://www.mib.com
[11] http://business.ftc.gov/documents/bus07-consumer-reports-what-insurers-need-know
[12] http://www.mib.com/request_your_record.html
[13] http://www.rxhistories.com/
[14] http://www.optum.com/health-plans/acquisition/manage-risk/rating-underwriting/medpoint-prescription-profiling.html
[15] https://www.privacyrights.org/fs/fsC4/CA-medical-prescription-privacy#pbm-prescription-privacy
[16] http://www.ftc.gov/opa/2007/09/ingenixmilliman.shtm
[17] https://www.privacyrights.org/consumer-guides/complete-list-consumer-guides#credit%20and%20credit%20reports
[18] http://www.rxhistories.com/RequestAReport/
[19] https://www.privacyrights.org/financial-privacy-how-read-your-opt-out-notices
[20] https://www.privacyrights.org/content/health-privacy-outside-healthcare-environment-health-records-job-available-government-and-cr
[21] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[22] http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/index.html
[23] https://www.privacyrights.org/california-medical-privacy
[24] https://www.privacyrights.org/is-your-health-privacy-protected-gray-areas
[25] http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/
[26] https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks
[27] https://oag.ca.gov/privacy/facts/medical-privacy/health-record
[28] http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3770
[29] http://www.worldprivacyforum.org/personal_health_records.html
[30] http://www.hhs.gov
[31] http://www.dol.gov
[32] http://www.dol.gov/
[33] http://www.dol.gov/dol/location.htm
[34] http://www.ftc.gov/bcp/edu/pubs/business/credit/bus08.shtm
[35] http://adata.org/
[36] http://www.adapacific.org/
[37] http://www.mbc.ca.gov/
[38] http://www.hmohelp.ca.gov
[39] https://www.ama-assn.org/
[40] https://www.worldprivacyforum.org/
[41] https://www.eff.org/issues/medical-privacy