

Employee Privacy Rights under HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to set a national standard for electronic transfers of health data. At the same time, Congress saw the need to address growing public concern about privacy and security of personal health data. The task of writing rules on privacy eventually fell to the U.S. Department of Health and Human Services (DHHS). After several modifications, DHHS issued the HIPAA Privacy Rule.

HIPAA Privacy rules apply to health care providers, health plan providers, and health care clearinghouses. These rules generally do not apply to most employer-employee interactions unless the employer is self-insured or is a health care provider, health plan provider, or health care clearinghouse that handles employee medical information.

The American's with Disabilities Act also provides protections with regard to employer access to employee medical information.

What kind of information is covered by the HIPAA Privacy Rule?

HIPAA covers any information about your past, present or future mental or physical health including information about payment for your care. To be covered by HIPAA, information has to be kept by a covered entity – a health care provider, health care plan, or health care clearinghouse. This, combined with some fact that identifies you (your name, address, telephone number, Social Security number) is called "protected health information" or PHI. PHI can be oral, handwritten, or entered into a computer. This means a conversation between a doctor and nurse about your condition has the same general protections as information written on your records.

Are there any limits on what can be disclosed from my medical file?

The Privacy Rule incorporates what it calls a "minimum necessary" standard when it comes to how much information should be disclosed. Doctors, hospitals, and others covered by the HIPAA Privacy Rule are required to limit the amount of information disclosed to others to the minimum necessary to accomplish the intended purpose.

What amounts to the minimum is left up to the health care provider, not you. And, the minimum necessary rule does not apply to information disclosed in connection with treatment. It also doesn't apply if you authorize the disclosure of your health information.

Your Health Records and Your Employer-----

For many people, the ultimate worry is that an employer's access to information about health and treatment or even the possibility of future illness can affect employment. The way and extent to which the HIPAA Privacy Rule covers your health information in the workplace depends on the type of health coverage you have. The majority of people in the workforce who have health benefits associated with employment fall into one of two categories:

* **Group health plans** are covered by the HIPAA Privacy Rule as long as the plan has 50 or more participants. If you are a member of a group health plan, your employer pays a premium to the health plan organization to cover your health care costs. In return for the premium paid, the health care plan assumes the risk of paying for health care expenses covered by the plan. The HIPAA Privacy Rule applies to the plan itself, but not your employer.

* **Self-insured plans** are health plans often offered by large employers as an employee benefit. Under self-insured health plans, the employer itself assumes the risk of health care costs and has the responsibility for paying health care claims out of the company's operating funds. Claims may be processed by company personnel or contracted out to other companies that process and maintain the records.

My employer sponsors a group health plan? Can my boss see my medical claims?

HIPAA says that the group health plan can tell your employer whether you are enrolled in the plan or not. Your employer can also get from the group plan what is called "summary" information to use to obtain premium bids or changes in coverage. If the health information your employer receives goes beyond the basic summary, then HIPAA requires the employer to establish procedures much like that of a covered entity. HIPAA attempts to limit the use of medical information for employment purposes.

My employer is self-insured. Does HIPAA guarantee my privacy?

Under the HIPAA Privacy Rule, an employer that is also the insurer of health benefits is in a category called a "hybrid" entity. That means the portion of the company's operations that deal with processing health claims is a covered entity. Like any other covered entity, a "hybrid" function must (1) give notice of written privacy procedures, (2) place restrictions on the use of health information, and (3) appoint a privacy officer and train staff.

Can my self-insured employer see my health claims?

If you are the least bit concerned about the privacy of your medical information, the close relationship between your boss and the person who processes your health claims can send a chill down your spine.

"It's Helen in personnel who's looking at all the forms, and knows whether you're seeing a psychiatrist, you just had your tubes tied, or you've just been diagnosed with cancer," quoting the chairman of the University of Massachusetts Medical School Psychiatry Department in *National Journal*, "Open Secrets," (Oct 9, 1999) at p.2880.

HIPAA requires that "hybrid" entities such as self-insured employers erect "firewalls" between the portion of the company that handles the health claims and the portion that does not. However, the effectiveness of this procedure remains to be seen. The threat to privacy posed by self-insured employers was the subject of a report prepared by Congressional Representative Henry Waxman in April, 2002, "Medical Privacy Policies of Large Corporations Have Major Deficiencies,"

www.house.gov/reform/min/pdfs/pdf_inves/pdf_privacy_rep.pdf.

My employer has an on-site health clinic. Is that covered by HIPAA?

An on-site health clinic at your place of employment may be another example of what the HIPAA Privacy Rule calls a "hybrid" entity. This depends on whether the health clinic transmits information electronically and engages in standard transactions under HIPAA's electronic data interchange rule, for example, if the clinic bills an employee's health plan.. If so, the records maintained by the health clinic are subject to the same protections that apply to other covered entities.

Are all records related to my employment and my health subject to HIPAA?

No. Records that relate to other employee benefits such as life insurance, disability, workers compensation, or long-term care insurance are not covered by HIPAA. Nor are records that relate to your employer's compliance with laws that govern safety and health risks in the workplace.

I work in a hospital. Is my employment file covered by HIPAA?

No. The Privacy Rule applies only to records maintained for treatment of patients. Records in your employment file are not covered.

What can I do if someone violates the HIPAA Privacy Rule?-

You don't have the right to sue under HIPAA. The most you can do is file a complaint. The privacy notice you receive from your health care provider or plan is required to tell you how to file a complaint within the organization. The notice should also tell you how to contact the DHHS Office of Civil Rights. This is the government office charged with enforcing the Privacy Rule.

You must file your complaint within 180 days of the violation, but DHHS can extend that time. HIPAA says you cannot be denied treatment because you file a complaint.

Even though the HIPAAA Privacy Rule does not give you the right to sue, other federal or state laws or regulations might give you the right to bring an action in court for violations of your privacy. If you feel your rights have been violated, you may want to discuss the situation with an attorney.

What happens after I complain?

The DHHS may decide to investigate and/or try to resolve the issue informally. A person or organization that is obliged to follow the Privacy Rule may face a civil fine of up to \$25,000. In extreme cases, the U.S. Department of Justice (DOJ) may be called in to conduct a criminal investigation. If the DOJ becomes involved, violators could face a jail term of up to 10 years and a fine of up to \$250,000.

Filing Complaints under HIPAA

U.S. Department of Health and Human Services (DHHS)

Office of Civil Rights

200 Independence Avenue, S.W.

Washington, D.C., 20201

(866) 627-7748

www.hhs.gov/ocr/hipaa/links.html

For the regional office nearest you, www.hhs.gov/ocr/hipaahealth.txt

Or email: OCRComplaint@hhs.gov

Source:

"Fact Sheet 8a: HIPAA Basics: Medical Privacy", Utility Consumers' Action Network / Privacy Rights Clearinghouse, April 2003.

www.privacyrights.org/fs/fs8a-hipaa.htm#3