1. Introduction

There is no one law that protects the privacy of all medical information in all situations. The Health Insurance Portability and Accountability Act (HIPAA) sets baseline rules for health information privacy. However, whether HIPAA applies at all depends on the situation. For more information on HIPAA privacy and security, see Privacy Rights Clearinghouse’s (PRC) Medical Privacy Fact Sheets.

In addition, privacy protections vary depending on the state law. In some instances there are no legal protections. This guide provides information on how, if at all, health information is protected in various settings where HIPAA may not apply.

2. Health records in the workplace

Whether and how the HIPAA Privacy Rule applies to an individual's health information in the workplace often depends on the type of health coverage the employee has.

a. How are group health plans different from self-insured health plans?

Most people who have health benefits associated with their job have one of two types of plans:

- **Group health plans.** The HIPAA Privacy Rule applies to group health plans as long as the plan has 50 or more participants. With a group health plan, the employer pays a premium to the health plan organization to cover 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 to the employer.
Self-insured plans. Often large employers offer self-insured health plans. Under self-insured 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 claims and maintain records.

i. May an employer who offers a group health plan see an employee’s medical claims?

HIPAA attempts to limit the use of medical information for employment purposes. A group health plan can tell an employer whether an employee is enrolled in the plan or not. In addition, an employer can get “summary health information” from the group plan to use to obtain premiums bids or changes in coverage. This is information that summarizes employees’ claims history, claims expenses, or types of claims experience under an employer-sponsored group plan. It counts no individual identifiers other than a five-digit zip code.

If an employer receives health information in addition to what constitutes a "summary," HIPAA requires the employer to establish procedures for protecting the data that are similar to what a covered entity [5] must do.

ii. Does HIPAA apply to an employer who offers a self-insured health plan?

Yes. Under the HIPAA Privacy Rule, an employer that also acts as a health plan by insuring employees’ health benefits is considered a “hybrid entity” [6]. That means the portion of the company’s operations that deal with processing health claims is a HIPAA-covered entity [5].

HIPAA requires hybrid entities such as self-insured employers to create firewalls between the portion of the company that handles health claims and the portion that does not. For example, a hybrid entity may not commingle medical claims data with personal records. Like any other covered entity, an employer functioning as a hybrid entity must (1) give written notice of privacy procedures (2) place restrictions on the use of health information and (3) appoint a privacy officer and train staff in proper privacy and security practices.

b. Does HIPAA apply to on-site employee health clinics?

An on-site employee health clinic may be subject to HIPAA as a hybrid entity [6] if it transmits information electronically and engages in standard transactions under the HIPAA electronic data interchange rule. For example, the on-site clinic may bill an employee’s health plan (which could be an employer-sponsored plan). If so, the records the health clinic maintains are subject to the same protections that apply to other covered entities.

c. Are all employment-related records that contain health information 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 an employer’s compliance with laws that govern safety and health risks in the workplace, such as the Occupational Safety and Health Act (OSHA) [7].

The federal Family and Medical Leave Act (FMLA) gives most workers the right to 12 weeks of unpaid leave per year for personal and family health. If an employee requests FMLA leave because of a serious illness, an employer may request a doctor's certification of the illness. However, an employer cannot require an employee to produce medical records. For more information, see the U.S. Department of Labor website [8].

In addition, many employers offer a variety of health and fitness programs, sometimes called Employee Health Programs (EHPs). Many are offered by outside companies that service multiple employers. EHPs may be as simple as lunchtime exercise or as structured as a plan that involves individualized diets, exercise plans, and close weight, blood pressure, and body mass index monitoring. Sometimes employees have access to mental health counselors or therapists. Such programs are generally not covered under HIPAA, and there isn't a universal privacy standard.

To learn more about health records and the workplace, see the HHS publication entitled Employers and Health Information in the Workplace [9].

d. Are hospital workers’ employment files covered by HIPAA?

No. HIPAA does not generally apply to employment records. In fact, the definition of protected health information [10] (PHI) specifically excludes employment records from the privacy protections of HIPAA.
However, HIPAA privacy protections would apply to a hospital employee’s records if he or she were admitted to the hospital as a patient.

e. Do individuals have rights with regard to employers asking for or using genetic information?

Yes. A federal law called the Genetic Information Nondiscrimination Act [11] (GINA) prohibits employers and insurance companies from treating a person differently or making a decision based on genetic information. The Equal Employment Opportunities Commission (EEOC), which enforces GINA, has information for consumers [12] about the Act and its application. Another good source, particularly from a privacy perspective, is the Council for Responsible Genetics [13].

3. Health records and the government

a. When may the government see an individual’s health information?

There are many situations in which the government has the right or a legal obligation to see an individual’s medical records without the individual’s permission. For example, state agencies must keep records of births and deaths as well as registries of people who have been diagnosed with serious illnesses such as cancer or HIV.

The HIPAA Privacy Rule applies to many government-sponsored health programs such as those covering active-duty military, veterans, and government employees. In addition, the Privacy Act of 1974 [14] (5 U.S.C. § 552a) applies to federal government agencies that collect personally identifiable health information. This means that federal agencies and contractors that are HIPAA-covered entities must follow the HIPAA Privacy Rule as well as the Privacy Act.

The U.S. Department of Health and Human Services [15] (HHS) is a federal government agency that may have access to health records. Typically, HHS would have this type of access when its Office for Civil Rights [16] (OCR) reviews complaints of alleged privacy violations. An individual might complain to OCR, for example, that her HMO refused to provide a copy of her medical records. OCR could then request a copy of the records from the HMO as part of its investigation.

In addition to investigating complaints, HHS also conducts privacy and security compliance audits. Both covered entities [5] and business associates [17] are subject to audits. To conduct the required audits, HHS contracts with a large accounting firm, but offers assurance that personal data disclosed during an audit is private and secure. Whether triggered by consumer complaints or audits, an HHS investigation will almost certainly mean that HHS and its contractors have access to some protected health information [10] (PHI). To read more about outside audits, see the HHS resource titled, Protection of Information Created or Obtained through the HIPAA Audit Program [18].

b. Do doctors send medical information to a government database?

According to HHS, there is no government database [19]. Nor are doctors required to deliver an individual’s health information to the government. An exception, as previously discussed, is for information required by HHS for enforcement purposes.

4. Health information and credit

a. Can medical-related debts be disclosed to a credit bureau?

Yes. When people receive care, they are patients. However, a patient can just as easily change roles and become a debtor. Patients are obligated to pay for any cost not covered by health insurance. All unpaid medical bills, like any other debt, may be reported to a credit bureau and result in a negative entry on a credit report and a lower credit score.

However, Fair Isaac Corporation (FICO), the private company that calculates consumer credit scores, changed the weight it gives medical bills in calculating a credit score when a consumer's credit record is otherwise clean [20]. The FICO 9 score recognizes that unpaid medical bills often have to do with billing errors and that people who are behind on medical bills are unlikely to be poor credit risk in general. The resulting FICO credit score will be higher. However, unpaid or delinquent medical bills will still appear on consumer credit reports, like those from Equifax, TransUnion, and Experian.

Remember: Patient consent is not required for providers to disclose information for “payment” purposes. For more information, see Privacy Rights Clearinghouse Fact Sheet 8b: The HIPAA Privacy Rule: How May Covered Entities Use and Disclose Health Information? [21]

HIPAA lists information that may be disclosed to a credit bureau such as:

• name and address;
b. Can a doctor or hospital give information about a patient to a collection agency?

Yes. A **covered entity** [5] may disclose information required to collect the debt but must also follow the “**minimum necessary**” [22] standard that applies to all disclosures under HIPAA. Debt collection is payment activity under HIPAA, and health providers should enter into a **business associate agreement** [17], which binds a debt collector to comply with HIPAA standards regarding the privacy and security of protected health information (PHI), before disclosing any information.

c. Do medical debt collectors have to comply with any laws?

Yes. Debt collectors, like all **business associates** [17], must comply with the HIPAA rules. In addition, business associates are subject to audit and the same penalties that apply to covered entities.

Debt collectors are also subject to the **Fair Debt Collection Practices Act** [23]. For more information about debt collection and privacy, see Privacy Rights Clearinghouse’s materials on debt collection [24].

d. Is it possible to dispute a medical bill?

Yes. Medical billing and insurance claims processes can be complicated and confusing. However, patients should make every attempt to stay on top of them. If a patient believes there is an error it is best to immediately dispute the matter in writing with the health provider and/or insurance company.

Patients who are unable to settle such disputes on their own may want to turn to a health care advocate, health care appraiser, or government agency in their state or local area. For example, California has a government agency, **The Office of Patient Advocate** [25], which accepts complaints, among other things, about billing disputes.

If a patient has a dispute regarding a hospital bill, the facility may have patient advocates on staff or have a connection to volunteer advocacy organizations that can help navigate the complex world of medical billing.

**Tip:** Make every effort to resolve billing errors before the debt is reported to a collection agency or the credit reporting agencies (Experian [26], Equifax [27], TransUnion [28]).

To learn more about consumer protection laws and rights regarding credit and collections see the following resources:

- Federal Trade Commission, Facts for Consumers, **Debt Collection FAQ** [29].
- Privacy Rights Clearinghouse Fact Sheet 6: **How Private is My Credit Report?** [30]
- Privacy Rights Clearinghouse Fact Sheet 27: **Debt Collection Practices: When Hardball Tactics Go Too Far** [31]
- Consumer Financial Protection Bureau, **Debt Collection: Questions and Answers** [32]

e. What is medical identity theft?

Medical identity theft is a unique form of fraud in which a thief receives medical care and/or benefits from someone else’s health insurer. It is essential to review all billings and insurance payments to make sure the charges apply to the correct patient. Victims of medical identity theft should follow the steps recommended by the **Federal Trade Commission** [33] or call the **Identity Theft Resource Center** [34] (a nonprofit that provides free victim assistance) at 888-400-5530. The California Attorney General also has helpful information in First Aid for Medical Identity Theft: Tips for Consumers [35], including different indications that you may be a victim, and how to respond.

f. Can an overdue medical bill appear on a credit report?

Yes. If neither the patient nor an insurer pays for the care, a medical debt can appear on a credit report. Under the **Fair Credit Reporting Act** [36], a credit report cannot reveal the name, address, or telephone number of a medical creditor unless the information is in code. According to credit bureau Experian, a **medical debt** [37] is identified as such with all other information removed. All information is, however, available when individuals order their own credit reports.

g. Can a healthcare provider check an individual’s credit report and credit score?
Like any other creditor, a provider or the provider’s debt collector may check credit reports of individuals who owe money for unpaid bills. A provider might also check an individual’s credit report if he or she applies for a free or discounted medical service. By checking a credit report, a provider or collector might learn, for example, that an individual has the ability to pay. For procedures that involve an extension of credit, the provider might decide whether someone presents a high risk for nonpayment.

5. Resources

Laws and Regulations

Health Information Technology for Economic and Clinical Health Act of 2009 [38] (HITECH)

Privacy Act of 1974 [39], 5 USC 552a

Genetic Information Nondiscrimination Act [40], Public Law 110-233

HHS Omnibus Rule [41], 78 Federal Register 5566 (January 25, 2013)

HHS Publications and Topics

Government data bases [19]

Employers and Health Information in the Workplace [9]

Health Information Technology [42]

Genetic Information [43]

Publications – Consumer Laws

Federal Trade Commission, Facts for Consumers, Debt Collection FAQ [29].

Consumer Financial Protection Bureau, Debt Collection: Questions and Answers [32]


Privacy Rights Clearinghouse Fact Sheet 27: Debt Collection Practices: When Hardball Tactics Go Too Far [31]


Links
[2] https://www.privacyrights.org/content/health-privacy-hipaa-basics
[3] https://www.privacyrights.org/Medical-Privacy
[5] https://www.privacyrights.org/content/health-privacy-hipaa-basics#covered%20entities
[6] https://www.privacyrights.org/content/health-privacy-hipaa-basics#hybrid%20entity
[10] https://www.privacyrights.org/content/health-privacy-hipaa-basics#privacy%20rule%20information
[17] https://www.privacyrights.org/content/health-privacy-hipaa-basics#business%20associate