



Privacy Rights Under the Health Insurance Portability and Accountability Act (HIPAA)

Did you know you have privacy rights when it comes to your health information as a patient? Read on to learn more about your privacy rights and the law that protects them.

1. What is the Health Insurance Portability and Accountability Act of 1996 (HIPAA)?

HIPAA is a federal law that protects sensitive patient health information from being shared without your permission (i.e. consent).

HIPAA protects protected health information, sometimes called individually identifiable health information.

2. What is protected health information (PHI)?

PHI is any and all information or data about your health and is considered private. PHI includes:

- Information your doctors, nurses, and other health care providers put in your medical record such as:
 - prescriptions
 - diagnoses
 - medical history
 - notes, evaluations, tests, etc.
- Conversations between you and your doctor about your medical care or treatment
- Information in your health insurer's computer system
- Billing information about you

3. Who has to follow HIPAA?

There are certain providers and programs that must follow HIPAA and protect your PHI. These generally include:

- Most health care providers. Examples of healthcare providers include doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists
- Health insurance companies
- Government programs that pay for health care, such as Medicare and Medicaid
- Health Care Clearinghouses (third party providers that manage medical claims)

4. Who does NOT have to follow HIPAA?

There are certain providers that HIPAA does not apply to. There may be other protections in place, however HIPAA generally does not cover:

- Life insurance
- Employers
- Most schools and school districts
- Many state agencies
- Most police departments
- Many state offices

5. Can a provider ever share my PHI without my consent?

There may be times a provider can share your PHI without your consent. Here are some ways your PHI may be shared without your consent:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their business
- For the protection of the public's health
- To make required reports to the police

6. What are some examples of HIPAA violations?

- A doctor sharing information with your family member about your diagnosis or lab results without your permission.
- A pharmacy sharing what medications you take with a friend without your permission
- A therapist sharing treatment information with another doctor without your permission

7. What are some examples of information that are NOT HIPAA violations?

Employee and education records are not considered PHI, so there is no HIPAA violation if this information is shared. However, there may be other laws that protect this information and may be violated if those records are shared.

8. How do I file a complaint?

If you believe your privacy rights have been violated under HIPAA, you may file a complaint with the Office of Civil Rights (OCR). For more information about HIPAA and the complaint process, visit [hhs.gov/hipaa](https://www.hhs.gov/hipaa) or call 800-368-1019

Do you have any more questions regarding this topic? If so, reach out to disAbility Law Center of Virginia. We can be reached by phone at 1-800-552-3962 (toll-free) or 804-225-2042 or you submit an online Get Help request at dlcv.org/get-help.