HIPAA Privacy Basics

Understand your obligations under HIPAA privacy rules for employer-sponsored health plans.

What HIPAA protects

HIPAA safeguards Protected Health Information (PHI) held by group health plans. Employers acting as plan sponsors must limit how PHI is used and disclosed.

Core employer obligations

- Maintain a Notice of Privacy Practices for the plan.
- Amend plan documents to describe permitted PHI uses.
- Establish administrative, physical, and technical safeguards.
- Appoint a privacy contact and train staff with PHI access.

Minimum necessary

Access and share only the least amount of PHI needed to accomplish a task. Keep employment records separate from plan PHI.

Breach response

- Investigate and document any suspected breach promptly.
- Notify affected individuals and HHS within required timeframes.
- Review safeguards to prevent recurrence.

Questions about how this applies to your organization? Our advisors offer a free consultation — visit the contact page on our website.

Educational use only — not legal or tax advice.