



# HIPAA Basics Compliance Checklist

*Compliance made simple — for small healthcare teams.*

---

## Why HIPAA Compliance Matters

Protecting patient privacy is more than a legal requirement — it's the foundation of trust between your practice and your patients.

HIPAA compliance safeguards Protected Health Information (PHI) through administrative, physical, and technical safeguards.

Following this checklist ensures your practice reduces breach risks, avoids costly fines, and demonstrates a culture of compliance that patients can rely on.

---

## Administrative Safeguards

- ☐ Privacy Officer and Security Officer designated in writing.
  - ☐ HIPAA policies and procedures current and accessible.
  - ☐ Annual HIPAA training completed for all staff.
  - ☐ Risk analysis conducted and documented within the past year.
  - ☐ Sanction policy exists and is communicated to all staff.
  - ☐ Business Associate Agreements (BAAs) executed and reviewed annually.
-

## **Technical Safeguards**

- ☐ Access to PHI restricted by job role.
  - ☐ Passwords updated regularly (minimum every 90 days).
  - ☐ Data encryption for email, EHR, and portable devices.
  - ☐ Audit logs enabled and reviewed routinely.
  - ☐ Two-factor authentication implemented where possible.
- 

## **Physical Safeguards**

- ☐ Workstations positioned to prevent public viewing of PHI.
  - ☐ Locked storage for paper records and devices containing PHI.
  - ☐ Visitor access restricted and logged.
  - ☐ Backup media stored securely offsite.
- 

## **Breach & Incident Response**

- ☐ Breach response plan established and reviewed annually.
  - ☐ All incidents documented and resolved promptly.
  - ☐ OCR breach reporting procedures known by staff.
- 

## **If These Are Not in Place — Do This**

If any of the safeguards above are not fully implemented:

- ☒ Schedule a brief compliance review to identify what's missing.
- ☒ Document all current gaps in your HIPAA program.
- ☒ Develop a short-term corrective action plan with deadlines.
- ☒ Train staff on updates or new processes within 30 days.
- ☒ Reach out to Guess Compliance Consulting for help with HIPAA assessments, templates, or staff training.

 *Compliance doesn't have to be complicated — take one small step today to build confidence and reduce risk.*

---

## Call to Action

♥ Ready to make HIPAA compliance simple? Visit <https://guesscomplianceconsultingllc.com>

---

© Guess Compliance Consulting LLC | <https://guesscomplianceconsultingllc.com>

Join our community: <https://facebook.com/groups/847852574359122>

*For educational purposes only. This resource is not legal advice.*