HIPAA IT checklist

For clinics and dental offices

1. Set scope and ownership

Use this worksheet to review electronic protected health information (ePHI), assign follow-up and document what you can verify. Mark items only when you can show the evidence. Review with your security official, privacy or compliance lead and counsel as appropriate. This is a planning aid, not legal advice, certification or a guarantee of compliance. Do not put patient names, credentials or other sensitive details on this worksheet.

- [ ] **Name the responsible security official.**
  Record the role responsible for developing and implementing security policies. Keep leadership, compliance and IT contacts current.

- [ ] **Map electronic health information.**
  Inventory where ePHI is created, received, maintained or transmitted. Include clinical records, imaging workstations, billing, hosted apps, file shares and remote access.

- [ ] **Identify vendors and agreements.**
  Determine which providers are business associates and confirm appropriate written agreements before allowing them to handle ePHI on your behalf. List who reviews these agreements.

- [ ] **Document a risk analysis.**
  Record risks and vulnerabilities to confidentiality, integrity and availability across the full ePHI scope. Document likelihood, impact and safeguards already in place.

- [ ] **Track risk-reduction decisions.**
  Assign each priority finding an owner and due date. Record decisions, remaining risk and changes that should trigger a reassessment.

Review date: _____ Reviewer role: _____

Follow-up owner and due date: _____

Do not record patient names, credentials or other sensitive information.

(406) 534-0911 · 2341 Broadwater Ave Ste D, Billings, MT 59102

HIPAA IT checklist

For clinics and dental offices

2. Verify people, devices and access

- [ ] **Review accounts against job responsibilities.**
  Check that access follows assigned roles. Document how staff and outside access are approved, changed and terminated. Review shared or unattended clinical workstations.

- [ ] **Verify user identification and emergency access.**
  Check that users have distinguishable IDs and that emergency access procedures work when the normal path is unavailable.

- [ ] **Check authentication and supported systems.**
  Verify that people or services seeking access are authenticated. Consider stronger approaches such as multifactor authentication based on risk. Assign an owner for updates and unsupported devices.

- [ ] **Review workstation, facility and device safeguards.**
  Review where workstations face patients or visitors, who can enter restricted areas and how devices and removable media are tracked, reused or disposed of.

- [ ] **Review encryption and transmission safeguards.**
  Evaluate safeguards for ePHI stored on systems and sent between them. Follow applicable current Security Rule implementation requirements and document addressable decisions. Addressable does not mean optional.

Review date: _____ Reviewer role: _____

Follow-up owner and due date: _____

Do not record patient names, credentials or other sensitive information.

(406) 534-0911 · 2341 Broadwater Ave Ste D, Billings, MT 59102

HIPAA IT checklist

For clinics and dental offices

3. Prove recovery and response

- [ ] **Verify audit controls and review records.**
  Confirm in-scope systems can record and support review of activity. Assign a reviewer, document exceptions and define escalation.

- [ ] **Exercise the contingency plan.**
  Verify backup, disaster recovery and emergency-mode operation plans. Test a representative restore with approved data and record what still depends on a third party or unavailable account.

- [ ] **Rehearse a suspected security incident.**
  Make sure staff know who to contact, what to report and where to record it. Involve the privacy lead in assessing whether breach notification is required. Do not wait for a routine review.

- [ ] **Check workforce security training.**
  Record what workforce members are taught about access, handling and reporting. Include people whose job changes or who work off site.

- [ ] **Evaluate work and maintain documentation.**
  Document policies, procedures and required records. Reevaluate safeguards when changes affect the ePHI environment and track the date and findings of the review.

Review date: _____ Reviewer role: _____

Follow-up owner and due date: _____

Do not record patient names, credentials or other sensitive information.

(406) 534-0911 · 2341 Broadwater Ave Ste D, Billings, MT 59102