HIPAA Compliance Checklist

*This checklist is provided for informational purposes only and does not constitute legal advice or a comprehensive HIPAA compliance solution.

1. Privacy Rule Compliance

- ☐ Designate a Privacy Officer

- ☐ Develop and implement privacy policies and procedures

- ☐ Conduct a thorough review of all uses and disclosures of PHI

- ☐ Implement appropriate safeguards to protect PHI

- ☐ Provide privacy training to all workforce members

- ☐ Develop and distribute a Notice of Privacy Practices

- ☐ Establish a process for individuals to request access to their PHI

- ☐ Create a process for amending PHI upon request

- ☐ Implement a system for tracking disclosures of PHI

- ☐ Establish agreements with Business Associates

2. Security Rule Compliance

☐ Designate a Security Officer

☐ Conduct a risk analysis of electronic PHI (ePHI)

☐ Implement appropriate administrative safeguards:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation

☐ Implement appropriate physical safeguards:

- Facility access controls
- Workstation use and security
- Device and media controls

☐ Implement appropriate technical safeguards:

- Access control
- Audit controls
- Integrity controls
- Transmission security

☐ Develop and implement security policies and procedures

☐ Regularly review and update security measures

3. Breach Notification Rule Compliance

- [ ] Develop and implement a breach notification policy

- [ ] Establish procedures for identifying and reporting breaches

- [ ] Create a process for assessing the probability of PHI compromise

- [ ] Develop templates for breach notifications

- [ ] Establish timelines for notifying individuals, HHS, and media (if applicable)

- [ ] Implement a system for documenting breach incidents and responses

4. Enforcement Rule Compliance

☐ Understand HIPAA enforcement processes and penalties

☐ Establish internal disciplinary policies for HIPAA violations

☐ Develop a process for responding to OCR investigations or audits

☐ Maintain documentation of all HIPAA compliance efforts

5. Organizational Requirements

- [ ] Conduct regular HIPAA compliance audits

  Implement a document retention policy

- [ ] Establish a process for updating policies and procedures

- [ ] Develop and maintain an inventory of systems containing PHI

- [ ] Implement a change management process for systems containing PHI

- [ ] Establish a process for managing Business Associate relationships

- [ ] Conduct regular workforce training on HIPAA compliance

6. Documentation and Record-Keeping

☐ Maintain all required HIPAA-related documentation for six years

☐ Document all policy and procedure reviews and updates

☐ Keep records of all training sessions and attendees

☐ Maintain logs of security incidents and breach notifications

☐ Document all risk assessments and mitigation efforts

7. Ongoing Compliance Management

- ☐ Schedule regular compliance committee meetings

- ☐ Stay informed about HIPAA updates and changes

- ☐ Conduct periodic reassessments of HIPAA compliance

- ☐ Implement a process for addressing compliance gaps

- ☐ Regularly review and update Business Associate Agreements

- ☐ Conduct annual HIPAA training for all workforce members

Ensure Your HIPAA Compliance with Gart Solutions

Navigating the complexities of HIPAA compliance can be challenging. Let GART, your trusted DevOps and cloud services provider, help you safeguard your patients' Protected Health Information (PHI) and ensure full compliance with HIPAA regulations.

Contact GART today to learn how we can assist you in:

- Conducting comprehensive risk assessments
- Implementing robust encryption and security measures
- Developing and managing Business Associate Agreements (BAAs)
- Providing ongoing training and support for your team

Reach out to Gart Solutions now and secure your peace of mind.

gart.

www gartsolutions.com

✉ info@gartsolutions.com