HIPAA Compliance Checklist for WordPress Websites

1. **Hosting Infrastructure**
    - Use a HIPAA-compliant hosting provider with signed BAA (e.g., Atlantic.Net, Amazon AWS with BAA).
    - Ensure hosting provider encrypts data at rest and in transit.
    - Verify physical and network security controls at the datacenter.
2. **Business Associate Agreements (BAA)**
    - Execute BAA with all service providers accessing or storing PHI (e.g., hosting, backups, email services).
    - Verify providers' HIPAA compliance posture before BAA execution.
3. **SSL/TLS**
    - Enforce HTTPS with TLS 1.2 or higher.
    - Redirect all HTTP traffic to HTTPS.
    - Use HSTS headers to prevent downgrade attacks.
4. **Authentication & Access Control**
    - Require strong passwords (min 12 characters, complexity rules).
    - Enforce Two-Factor Authentication (2FA) for all users.
    - Limit admin access by role, principle of least privilege.
    - Audit and remove inactive user accounts regularly.
5. **Audit Logging**
    - Enable logging for all access and administrative actions.
    - Retain logs securely for at least 6 years.
    - Use plugins like WP Activity Log with offsite log storage.
6. **Data Encryption**
    - Encrypt all PHI at rest using server-level or disk-level encryption.
    - Use encrypted backup solutions with secure key management.
7. **Form Handling & PHI Transmission**
    - Use HIPAA-compliant form plugins (e.g., Formidable Forms with HIPAA add-on).
    - Do not send PHI over email without encryption.
    - Ensure data transmission is over TLS-only endpoints.
8. **Database Security**
    - Harden MySQL/PostgreSQL with firewall rules, non-default ports, and encrypted connections.
    - Sanitize all user inputs to prevent SQL injection.
    - Remove direct DB access for web users (use prepared statements, ORM).
9. **Firewall & Intrusion Protection**
    - Enable Web Application Firewall (e.g., Cloudflare WAF, Wordfence Premium).
    - Block all unnecessary ports and protocols at the server firewall.
    - Geo-limit and rate-limit access to admin URLs.
10. **Malware & Vulnerability Scanning**

- Schedule automated scans (Sucuri, Wordfence).
- Monitor file changes and flag unauthorized modifications.
- Perform routine manual code audits of custom themes/plugins.

11. **Backup & Recovery**

- Implement encrypted, versioned, offsite backups.
- Automate daily backups of files and database.
- Test recovery from backup at regular intervals.

12. **Session & Cookie Security**

- Enable `HttpOnly`, `Secure`, and `SameSite=Strict` for all cookies.
- Limit session lifespan; auto-logout inactive users.
- Store sessions server-side if custom logic handles PHI.

13. **Data Retention & Disposal**

- Create and follow retention policies for PHI.
- Securely delete outdated records from DB and backups.
- Ensure secure wiping of retired storage devices.

14. **Privacy Policy & Notices**

- Publish HIPAA-compliant privacy policy.
- Inform users how PHI is used, stored, and protected.
- Display notice of privacy practices as required.

15. **Training & Awareness**

- Conduct regular HIPAA training for admins and content managers.
- Document compliance practices and audit processes.

16. **Security Risk Analysis**

- Perform regular risk assessments of the entire WordPress environment.
- Document identified risks and remediation actions.