SOFTSOLS · FREE CHECKLIST

HIPAA-Compliant App Development Checklist

A practical pre-launch checklist for founders, product owners and engineering teams building healthcare apps for the US market.

How to use it: work through each section with your engineering lead and compliance advisor. Every unchecked item is a gap to close before you handle real patient data.

1. Scope and agreements

- ☐ Confirm whether your app creates, receives, stores or transmits protected health information (PHI) for a covered entity or business associate.
- ☐ Map every place PHI flows: mobile app, web app, APIs, databases, backups, logs, analytics, email and support tools.
- ☐ Sign a Business Associate Agreement (BAA) with every vendor that handles PHI: cloud host, database, email/SMS, video, AI model provider and support desk.
- ☐ Use only HIPAA-eligible services within your cloud provider and configure them as their documentation requires.
- ☐ Keep analytics, crash reporting and marketing pixels free of PHI.

2. Risk analysis and policies

- ☐ Complete and document a security risk analysis before launch and whenever the system changes significantly.
- ☐ Write security policies covering access, passwords, devices, incident response, backups and data retention.
- ☐ Name a security officer responsible for the program.
- ☐ Train everyone with PHI access and keep training records.

3. Access control

- ☐ Unique user IDs for every person; no shared accounts.
- ☐ Role-based access so users see only the minimum PHI they need.
- ☐ Multi-factor authentication for clinicians, admins and all production and cloud-console access.
- ☐ Automatic session timeout and logout on shared devices.
- ☐ Emergency ("break glass") access procedure, logged and reviewed.
- ☐ Prompt removal of access when staff leave or change roles; quarterly access reviews.

4. Encryption and data protection

- ☐ TLS 1.2+ for all data in transit, including internal service-to-service traffic.
- ☐ Encryption at rest for databases, file storage, backups and mobile device storage.
- ☐ Managed key storage (for example AWS KMS or Azure Key Vault); no keys or secrets in source code.

- ☐ Avoid PHI in URLs, push-notification text, logs and error messages.
- ☐ Secure deletion and a documented retention schedule.

5. Audit controls and monitoring

- ☐ Log every create, read, update and delete of PHI with user, time and record.
- ☐ Protect logs from tampering and retain them per your policy.
- ☐ Alert on suspicious activity: repeated failed logins, unusual exports, privilege changes.
- ☐ Review audit logs on a regular schedule and document the reviews.

6. Application security

- ☐ Secure coding standards and peer code review for every change.
- ☐ Dependency and container vulnerability scanning in CI/CD.
- ☐ Input validation and protection against OWASP Top 10 risks.
- ☐ Annual penetration test by a qualified third party, plus a test before major releases.
- ☐ For AI features: no PHI sent to models without a BAA, prompt-injection safeguards, and human review of clinical outputs.

7. Availability and incident response

- ☐ Automated backups with tested restores.
- ☐ Disaster recovery plan with defined recovery time and recovery point objectives.
- ☐ Incident response plan that includes breach assessment and HIPAA Breach Notification Rule timelines.
- ☐ Contact list for legal counsel, vendors and the security officer.

8. Patient-facing features

- ☐ Clear privacy notice and consent capture where required.
- ☐ Patient identity verification before sharing records.
- ☐ Secure messaging instead of standard email or SMS for PHI.
- ☐ Telehealth sessions encrypted end to end with a BAA-covered video provider.

Need help closing the gaps?

Softsols builds HIPAA-ready web and mobile apps, patient portals, telehealth and billing software for US healthcare organizations. Book a free consultation at softsols.pk/request-a-quote.

This checklist is general guidance, not legal advice. Consult a qualified HIPAA attorney or compliance professional about your specific obligations.