HIPAA Software Readiness Checklist

For healthcare founders and product teams reviewing software before building, buying, or scaling systems that may touch protected health information.

Use this for technical discovery. It is not legal advice, a compliance certificate, or a replacement for a formal HIPAA risk analysis. Use it to organize PHI flows, vendor scope, access, logs, cloud, AI, analytics, backup, and delivery questions before architecture hardens.

Source basis: HHS guidance on the HIPAA Security Rule, Security Rule summary, and covered entities/business associates.

READINESS REVIEW

1. Covered workflow Identify whether the product supports care, payment, operations, clinical documentation, patient communication, insurance, provider workflows, or another healthcare function.	**2. PHI data map** List where PHI is created, received, maintained, transmitted, transformed, exported, deleted, logged, backed up, or viewed by support users.
3. Vendor and BAA scope Review cloud, email, SMS, AI, analytics, monitoring, storage, search, support, video, and data-processing vendors for BAA availability and covered features.	**4. Identity and roles** Define patient, clinician, staff, admin, support, service-account, and emergency-access roles with least-privilege permissions and reviewable access history.
5. Tenant and account boundaries Decide how organizations, clinics, practices, departments, patients, and internal users are separated across application data, storage, queues, caches, and jobs.	**6. Environments** Separate development, staging, and production. Prefer synthetic data outside production, and govern any production-derived subset with access limits and expiry.
7. Encryption and secrets Check transport security, encryption at rest, key ownership, secret storage, rotation, workload identity, break-glass access, and recovery paths.	**8. Audit evidence** Capture meaningful access, administrative, deployment, data-change, vendor, and support events without placing unnecessary PHI into logs.
9. Analytics and monitoring Design allowlisted event names and technical identifiers. Review URLs, breadcrumbs, stack traces, replay tools, exports, alerts, and integrations for PHI leakage.	**10. AI and automation** Map prompts, files, transcripts, embeddings, logs, model retention, subprocessors, human review, failure modes, and whether the AI service is covered by the right agreement.
11. Backup and recovery Set recovery objectives, protect backup access, test restore paths, document retention, and verify deletion expectations across derived and backup copies.	**12. Delivery readiness** Review CI/CD permissions, protected releases, artifact provenance, dependency scanning, database migrations, rollback plans, and emergency deployment ownership.

DECISION NOTES

What data is in scope?	Specific PHI categories, files, identifiers, events, and derived data the product may handle.	Notes:
Who is responsible?	Product, engineering, security, privacy, legal, support, and vendor-review owners before launch pressure arrives.	Notes:

Which vendors can receive what?	Approved services, covered features, retention settings, subprocessors, and data that must never be sent.	Notes:
What evidence proves the controls?	Audit trails, access reviews, restore tests, incident runbooks, release records, and deletion checks.	Notes:
What remains unresolved?	Legal review items, architecture decisions, vendor gaps, manual workflows, and post-launch controls.	Notes:

USEFUL FOLLOW-UP

Bring this to the first architecture conversation with the workflow, current stack, intended vendors, target timeline, and the highest-risk data path you already know. Do not send PHI, patient records, credentials, keys, screenshots containing patient data, or incident evidence by email.

Project review: https://anqureshi.com/contact?utm_source=hipaa_checklist_pdf&utm;_medium=document&utm;_campaign=project_inquiry