HIPAA COMPLIANCE

FOR INDIAN HEALTHCARE STARTUPS

Your Complete Checklist — 2026 Edition

Covering Privacy Rule • Security Rule • Breach Notification • Indian Dual Compliance

Prepared by Bithost | ZHOST Consulting Private Limited | sales@bithost.in

v1.0 • February 2026 • 17 Sections • 220+ Controls • Not Legal Advice

⚠ Important Disclaimer

This checklist is a practical compliance guide based on HIPAA regulations (45 CFR Parts 160 and 164) and does not constitute legal advice. Indian healthcare startups handling US patient data must also comply with the DPDP Act 2023, IT Act 2000, and other applicable Indian regulations. Consult qualified US healthcare legal counsel and Indian technology law counsel before finalizing your compliance programme.

PRIORITY KEY	
CRITICAL	Non-negotiable. Absence represents direct HIPAA violation or immediate breach risk.
HIGH	Must be in place before handling any PHI in production.
MEDIUM	Important control. Address within 30 days of initial deployment.
LOW	Best practice. Resolve within 90 days on your compliance roadmap.

✓	Checklist Item	What to Check / Notes	Priority
1 | HIPAA APPLICABILITY & INDIAN REGULATORY CONTEXT			
Understanding When HIPAA Applies to Indian Startups			
☐	**Determine If HIPAA Applies to Your Business**	HIPAA applies if you handle PHI of US patients, work with US-based Covered Entities, or offer services to US health insurers or providers.	CRITICAL
☐	**Identify Your Role: Covered Entity or Business Associate**	CE = direct healthcare provider/insurer. BA = vendor/partner processing PHI on CE's behalf. Indian startups are usually BAs.	CRITICAL
☐	**Review All US Client Contracts for HIPAA Requirements**	Many US health tech contracts mandate HIPAA compliance as a condition of engagement.	HIGH
☐	**Map Which Products/Features Touch US Patient Data**	Not every product line may be in scope. Document scope precisely.	HIGH
☐	**Understand HIPAA Does Not Replace Indian Law**	You must comply with HIPAA AND DPDP Act 2023, IT Act 2000, and MoHFW guidelines simultaneously.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Obtain Formal Legal Opinion on HIPAA Applicability**	Jurisdiction and applicability can be complex. Get legal counsel opinion in writing.	HIGH
	Dual Compliance: HIPAA + Indian Regulations		
☐	**Map HIPAA Controls to DPDP Act 2023 Requirements**	Many controls overlap. Document where they align and where they diverge.	HIGH
☐	**Comply with IT (Amendment) Act 2008 on Sensitive Personal Data**	SPDI Rules 2011 govern health data. HIPAA stricter in most areas; follow the higher standard.	HIGH
☐	**Review ABDM (Ayushman Bharat Digital Mission) Guidelines**	If integrating with ABHA/ABDM, additional Indian health data requirements apply.	MEDIUM
☐	**Understand Cross-Border Data Transfer Restrictions**	DPDP Act 2023 restricts transfers to certain countries. Verify US is an approved destination.	HIGH
☐	**Review IRDAI Guidelines if Handling Insurance Data**	Health insurance data processed for Indian insurers has separate regulatory requirements.	MEDIUM
☐	**Document Your Dual Compliance Framework Formally**	Single policy document showing how controls satisfy both frameworks simultaneously.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
	2 | BUSINESS ASSOCIATE AGREEMENTS (BAA)		
	BAA Basics & Execution		
☐	**Sign a BAA with Every US Covered Entity You Serve**	No BAA = no business. This is non-negotiable under HIPAA. One per client/partner.	CRITICAL
☐	**Review BAA Terms Before Signing — Do Not Auto-Accept**	BAAs assign significant liability. Legal review mandatory before execution.	CRITICAL
☐	**Ensure BAA Covers All Services You Provide**	Scope must match actual data flows. Mismatched scope creates compliance gaps.	HIGH
☐	**Maintain a Central Register of All Executed BAAs**	BAA log with counterparty, date, scope, review date, and signatory.	HIGH
☐	**Set BAA Review Reminders Every 2 Years**	Business relationships and data flows change. BAAs must stay current.	MEDIUM
☐	**Obtain BAAs from All Your Sub-Processors Touching PHI**	You are responsible for your subcontractors. No BAA with them = HIPAA violation.	CRITICAL
	BAA Substance & Sub-BA Management		
☐	**Verify BAA Contains All 45 CFR 164.504(e) Required Elements**	Permitted uses, safeguards, breach reporting, agent restrictions, termination terms.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Ensure BAA Requires Sub-BAs to Match Your HIPAA Obligations**	Flow-down requirements must cascade to every vendor touching PHI.	HIGH
☐	**Include Breach Notification Timelines in BAA**	Typically requires reporting to CE within 60 days. Negotiate shorter windows if possible.	HIGH
☐	**Confirm BAA Addresses PHI Return or Destruction on Termination**	At contract end, PHI must be returned or securely destroyed. Document the process.	HIGH
☐	**Get US-Qualified Legal Review of BAA Template**	Indian counsel may miss HIPAA-specific nuances. US healthcare attorney review is worth it.	HIGH
☐	**Register All Sub-BAs in Your Third-Party Risk Register**	Track which sub-BAs touch PHI, what their BAA covers, and when it was last reviewed.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
3 | PHI IDENTIFICATION & DATA MAPPING			
What Counts as PHI			
☐	**Train Team on All 18 HIPAA PHI Identifiers**	Name, DOB, address, phone, email, SSN, MRN, account numbers, IP address, photos, and more.	CRITICAL
☐	**Conduct a Full PHI Data Discovery Across All Systems**	Where does PHI live? Databases, file stores, logs, backups, email, Slack, code repos.	CRITICAL
☐	**Identify PHI in All Its Forms: Electronic, Paper, Verbal**	ePHI is the focus for IT, but physical and verbal PHI also have safeguard requirements.	HIGH
☐	**Check Log Files and Monitoring Systems for PHI**	Application logs routinely capture PHI without developers realizing it.	HIGH
☐	**Check Analytics and Reporting Pipelines for PHI**	BI tools, dashboards, and data exports often carry PHI from production systems.	HIGH
☐	**Document PHI in AI/ML Training Datasets**	If you trained models on patient data, that data is still PHI regardless of how it's used.	CRITICAL
Data Flow Mapping			
☐	**Create and Maintain a PHI Data Flow Diagram**	Show every system, every hop, every integration where PHI travels.	CRITICAL
☐	**Map PHI Flows Across All Third-Party Integrations**	Every API, webhook, and data export to external systems must be mapped.	HIGH
☐	**Identify All Countries Where PHI Is Stored or Processed**	Data residency matters. Document every region and datacenter holding PHI.	HIGH
☐	**Map PHI Retention Periods in Every System**	How long is PHI in each database, cache, backup, and archive?	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Update Data Flow Map After Every Architectural Change**	New feature, new integration, new vendor = data map update required.	HIGH
☐	**Review Data Flow Map in Every Compliance Audit**	Auditors will ask for this. Keep it current and version-controlled.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
4 | HIPAA PRIVACY RULE COMPLIANCE			
Minimum Necessary Standard			
☐	**Apply Minimum Necessary Standard to All PHI Access**	Only access, use, or disclose the minimum PHI needed for the specific purpose.	CRITICAL
☐	**Design Role-Based Access So Roles Only See PHI They Need**	A billing team member should not see clinical notes. Enforce at the data layer.	HIGH
☐	**Apply Minimum Necessary to API Responses**	APIs returning PHI should return only the fields the requester is authorized to receive.	HIGH
☐	**Enforce Minimum Necessary in Analytics and Reporting**	Reports should use de-identified or aggregated data wherever the use case allows.	HIGH
☐	**Document Minimum Necessary Policies for Each Use Case**	Written justification for each class of PHI access and why the minimum is met.	MEDIUM
Permitted Uses & Disclosures			
☐	**Document All Permitted Uses of PHI Your Business Makes**	Treatment, payment, operations, and any other use must be documented and justified.	HIGH
☐	**Obtain Patient Authorization for Non-Standard PHI Uses**	Marketing, research, or non-standard disclosures require explicit patient authorization.	HIGH
☐	**Never Use PHI for Marketing Without Explicit Authorization**	Selling PHI or using it for unsolicited marketing is a HIPAA violation and a criminal offence.	CRITICAL
☐	**Document Each PHI Disclosure in a Disclosure Accounting Log**	Required for disclosures outside treatment, payment, and operations.	HIGH
☐	**Apply De-identification Before Using PHI for Analytics**	Safe Harbor method (remove all 18 identifiers) or Expert Determination method.	HIGH
☐	**Establish a Process to Handle Patient Rights Requests**	Right of access, right to restrict, right to amend — response timelines apply.	HIGH
Notice of Privacy Practices			
☐	**Publish a HIPAA-Compliant Notice of Privacy Practices**	Required if you are a Covered Entity. If BA, ensure your CE clients have valid NPPs.	HIGH
☐	**Ensure NPP Describes All Uses and Disclosures Accurately**	NPP must accurately reflect actual data practices. Mismatches are violations.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Translate NPP for Non-English Speakers If Required**	If serving populations with limited English proficiency, translation may be required.	MEDIUM
☐	**Update NPP When Privacy Practices Change**	Material changes require NPP update and redistribution.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
5 | HIPAA SECURITY RULE — ADMINISTRATIVE SAFEGUARDS			
Security Management			
☐	**Conduct and Document a Formal Risk Analysis**	The most cited HIPAA violation. Written risk analysis covering all ePHI systems is mandatory.	CRITICAL
☐	**Implement a Risk Management Plan Addressing All Identified Risks**	Written plan with assigned owners, timelines, and remediation actions.	CRITICAL
☐	**Assign a Designated HIPAA Security Officer**	One person responsible for security policy development and implementation.	CRITICAL
☐	**Assign a Designated HIPAA Privacy Officer**	Can be the same person as Security Officer at small startups. Must be formally designated.	CRITICAL
☐	**Conduct Annual Risk Analysis Reviews**	Risk landscape changes. Annual review is the minimum; major changes trigger interim review.	HIGH
☐	**Document All Security Decisions and Their Justifications**	HIPAA requires demonstrating reasonable and appropriate measures. Document everything.	HIGH
Workforce & Training			
☐	**Conduct HIPAA Training for All Workforce Members**	Everyone who touches ePHI or has any access to systems holding ePHI.	CRITICAL
☐	**Complete Training Before Granting Access to ePHI Systems**	New hires must complete HIPAA training before day-one system access.	CRITICAL
☐	**Conduct Annual HIPAA Refresher Training**	Yearly refresher with acknowledgement. Document attendance and completion.	HIGH
☐	**Implement Sanction Policy for HIPAA Policy Violations**	Written sanctions: verbal warning, written warning, termination. Apply consistently.	HIGH
☐	**Screen Workforce Members Handling PHI (Background Checks)**	Especially for roles with access to sensitive PHI. Document screening process.	HIGH
☐	**Conduct Role-Specific HIPAA Training for Technical Roles**	Developers and DevOps need training on ePHI handling in code, logs, and infrastructure.	HIGH
☐	**Document All Training Completions with Signatures**	Training records must be retained for 6 years. Name, date, topic, acknowledgement.	HIGH
Access Management			

✓	Checklist Item	What to Check / Notes	Priority
☐	**Implement Access Authorization Procedures for ePHI Systems**	Formal process to grant, modify, and revoke access. No informal access grants.	CRITICAL
☐	**Conduct Access Reviews for ePHI Systems Quarterly**	Review who has access, whether they still need it, and whether access is appropriate.	HIGH
☐	**Revoke ePHI Access Within 24 Hours of Termination**	Immediate revocation on separation. Verify across all systems including backups.	CRITICAL
☐	**Maintain Access Logs for All ePHI Systems**	Who accessed what, when, from where. Retain logs for 6 years.	HIGH
☐	**Implement Clearance Procedures for Role Changes**	Promotion or role change may alter required access. Revoke old, grant new.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
6 | HIPAA SECURITY RULE — PHYSICAL SAFEGUARDS			
Facility & Workstation Controls			
☐	**Implement Physical Access Controls to Facilities Holding ePHI**	Key cards, biometrics, sign-in logs for server rooms and offices accessing ePHI.	HIGH
☐	**Maintain Visitor Logs for Areas Where ePHI Is Accessible**	Log every visitor entry and exit in secure areas.	HIGH
☐	**Ensure Workstations Accessing ePHI Are in Secured Locations**	No ePHI access from open public areas, shared coworking without controls.	HIGH
☐	**Position Screens to Prevent Shoulder-Surfing**	Screens with PHI must not be visible to unauthorized persons.	MEDIUM
☐	**Implement Automatic Screen Lock on All ePHI Workstations**	Maximum 5-minute idle timeout before screen locks.	HIGH
☐	**Enforce Clean Desk Policy for PHI Documents**	No physical PHI documents left on desks when workstation unattended.	MEDIUM
Device & Media Controls			
☐	**Maintain Inventory of All Devices Accessing ePHI**	Every laptop, phone, tablet, server — tracked by asset tag.	HIGH
☐	**Encrypt All Devices That Store or Access ePHI**	Full-disk encryption on all laptops and mobile devices. Verify it is on, not just enabled.	CRITICAL
☐	**Implement Remote Wipe for All Mobile Devices Accessing ePHI**	MDM enrolled. Wipe capability tested annually.	HIGH
☐	**Define and Follow Secure Disposal Procedures for ePHI Media**	NIST 800-88 standards. Certificate of destruction for drives and devices.	HIGH
☐	**Restrict Use of Removable Media (USB) on ePHI Systems**	Block or monitor USB use. Any ePHI on removable media must be encrypted.	HIGH
☐	**Document Media Movement and Re-Use Procedures**	Tracking when media containing ePHI is moved between locations.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
☐	**Disable Unnecessary Ports on ePHI Workstations**	Bluetooth, unused USB ports — disable where not operationally needed.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
7 | HIPAA SECURITY RULE — TECHNICAL SAFEGUARDS			
Access Control			
☐	**Assign Unique User IDs to Every Workforce Member**	No shared accounts for any system holding ePHI. One person, one identity.	CRITICAL
☐	**Implement Multi-Factor Authentication for All ePHI System Access**	MFA on every application, VPN, cloud console, and database with ePHI.	CRITICAL
☐	**Enforce Automatic Logoff After Inactivity (15 Minutes Maximum)**	Session timeout on all ePHI applications and systems.	HIGH
☐	**Implement Emergency Access Procedures for ePHI**	Break-glass access with audit trail for emergency situations.	HIGH
☐	**Apply Encryption to All ePHI at Rest**	AES-256 minimum. Every database, file store, and backup encrypted.	CRITICAL
☐	**Enforce Role-Based Access Control on ePHI Databases**	Database-level access controls aligned with job function and minimum necessary.	HIGH
☐	**Disable Default Passwords on All Systems Holding ePHI**	Default credentials are a primary breach vector. Change on first deployment.	CRITICAL
Audit Controls & Integrity			
☐	**Enable Audit Logging on All ePHI Systems**	Log every access: who, what, when, from where. Immutable and centralized.	CRITICAL
☐	**Retain Audit Logs for Minimum 6 Years**	HIPAA documentation retention requirement. Logs are documentation.	CRITICAL
☐	**Implement Tamper-Evident Log Storage**	Logs must not be modifiable by the systems that generated them.	HIGH
☐	**Review Audit Logs for Unauthorized Access Weekly**	Automated alerts plus manual review. Unauthorized access detection is mandatory.	HIGH
☐	**Implement ePHI Integrity Controls**	Hash verification, checksums, or digital signatures to detect unauthorized modification.	HIGH
☐	**Monitor for ePHI Exfiltration Patterns in Audit Logs**	Large data exports, off-hours access, bulk downloads — alert and investigate.	HIGH
Transmission Security			
☐	**Encrypt All ePHI in Transit with TLS 1.2 or Higher**	No ePHI transmitted over unencrypted channels. TLS 1.3 preferred.	CRITICAL
☐	**Use End-to-End Encryption for ePHI in Messaging Systems**	Standard SMS and email do not meet HIPAA transmission requirements.	CRITICAL
☐	**Validate TLS Certificates on All ePHI API Endpoints**	Certificate pinning or strict certificate validation for high-sensitivity integrations.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Prohibit ePHI Transmission via Non-Approved Channels**	No PHI via personal email, WhatsApp, or unauthorized file-sharing services.	CRITICAL
☐	**Encrypt Backups Containing ePHI Before Transmission**	Backup transfers must use encrypted channels and encrypted payloads.	HIGH
☐	**Document All Approved ePHI Transmission Methods**	Written policy listing approved channels, encryption standards, and acceptable use.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
8 | CLOUD INFRASTRUCTURE & HOSTING COMPLIANCE			
Cloud Provider Selection & Configuration			
☐	**Use Only HIPAA-Eligible Cloud Services for ePHI Workloads**	AWS, Azure, GCP each publish lists of HIPAA-eligible services. Stay within that list.	CRITICAL
☐	**Execute BAA with Your Cloud Provider**	AWS, Azure, GCP all offer HIPAA BAAs. Sign one before storing any ePHI.	CRITICAL
☐	**Enable Encryption at Rest for All Cloud Storage Holding ePHI**	S3, RDS, EBS, Azure Blob, GCS — all encrypted with customer-managed keys.	CRITICAL
☐	**Enable Encryption in Transit for All Cloud Services**	Force TLS. Disable non-encrypted endpoints. Verify with configuration audit.	CRITICAL
☐	**Enable Audit Logging for All Cloud Account Activity**	AWS CloudTrail, Azure Monitor, GCP Audit Logs — enabled for all accounts.	CRITICAL
☐	**Restrict PHI Workloads to Specific Approved Cloud Regions**	Know where data sits. Avoid regions in countries with data sovereignty conflicts.	HIGH
☐	**Enable Cloud Security Posture Management (CSPM)**	AWS Security Hub, Azure Defender, GCP Security Command Center — continuous monitoring.	HIGH
Network & Access Security			
☐	**Place ePHI Databases in Private Subnets**	No direct internet access to any database holding PHI.	CRITICAL
☐	**Enforce VPN for Remote Access to ePHI Systems**	No direct RDP or SSH to ePHI servers over the internet.	HIGH
☐	**Implement Network Segmentation Between PHI and Non-PHI Workloads**	PHI systems isolated from general workloads. Separate VPCs/VNets.	HIGH
☐	**Enable Web Application Firewall on All PHI-Facing Applications**	OWASP rule sets and managed rules. Block common attack patterns.	HIGH
☐	**Conduct Quarterly Cloud Security Configuration Reviews**	Check for configuration drift. Every quarter minimum.	HIGH
☐	**Remove All Publicly Accessible Cloud Storage Holding ePHI**	No public S3 buckets, Azure blobs, or GCS buckets with PHI. Ever.	CRITICAL
☐	**Enable DDoS Protection on PHI-Facing Applications**	Healthcare availability is patient safety. Protect against availability attacks.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
9 | APPLICATION SECURITY FOR HEALTHCARE APPS			
Secure Development Practices			
☐	**Train All Developers on HIPAA-Specific Secure Coding Practices**	OWASP Top 10, injection prevention, encryption in code, PHI logging risks.	HIGH
☐	**Conduct Threat Modeling for All Features Handling PHI**	STRIDE or similar before building. Identify PHI exposure paths at design.	HIGH
☐	**Implement Static Application Security Testing in CI/CD**	SAST scans on every pull request. Block merges with HIGH/CRITICAL findings.	HIGH
☐	**Conduct Dynamic Application Security Testing on PHI-Handling Endpoints**	DAST scans against staging before every major release.	HIGH
☐	**Enforce Code Review with HIPAA Security Checklist**	Code reviewers explicitly check for PHI handling issues in every PR.	HIGH
☐	**Prohibit PHI in URL Parameters or Query Strings**	URLs are logged everywhere. PHI in URLs = PHI in dozens of log systems.	CRITICAL
☐	**Sanitize All Error Messages — Never Return PHI in Errors**	Stack traces, error objects, and API error responses must never contain PHI.	HIGH
API & Integration Security			
☐	**Require Authentication and Authorization on All PHI APIs**	No unauthenticated endpoints that can return PHI under any condition.	CRITICAL
☐	**Implement OAuth 2.0 / SMART on FHIR for Health API Auth**	Industry standard for healthcare interoperability. Required for FHIR APIs.	HIGH
☐	**Rate-Limit All PHI-Returning API Endpoints**	Prevent bulk PHI extraction via repeated API calls.	HIGH
☐	**Log All API Access to PHI with Full Audit Context**	User identity, timestamp, resource accessed, response code.	HIGH
☐	**Validate FHIR Resource Schemas Before Processing**	Malformed FHIR resources can cause processing errors that expose PHI.	MEDIUM
☐	**Apply Field-Level Encryption for Highly Sensitive PHI Fields**	SSN, diagnosis codes, mental health data — encrypt at the field level.	HIGH
☐	**Implement API Gateway with WAF for All External PHI APIs**	Single controlled entry point with logging, rate limiting, and threat detection.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
10 | BREACH NOTIFICATION & INCIDENT RESPONSE			
Breach Definition & Assessment			
☐	**Train Team on HIPAA Definition of a Breach**	Unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises security/privacy.	CRITICAL

✓	Checklist Item	What to Check / Notes	Priority
☐	**Establish a Breach Risk Assessment Process**	Four-factor test: nature of PHI, who accessed, whether accessed, mitigation extent.	CRITICAL
☐	**Document Every Potential Breach Even If Assessed as Not a Breach**	Your documentation must show you considered and ruled out breach status.	HIGH
☐	**Treat Encrypted PHI Loss as Low-Risk (With Conditions)**	Loss of properly encrypted PHI with no key compromise is not a reportable breach.	MEDIUM
☐	**Establish Breach Categorization Criteria**	Define what constitutes low, medium, high severity breach for your context.	HIGH
	Notification Requirements & Process		
☐	**Notify Covered Entity Business Partner Within 60 Days of Discovery**	Most BAAs require faster notification. Check your specific BAA terms.	CRITICAL
☐	**Notify HHS of Breaches Affecting 500+ Individuals Within 60 Days**	Submit to HHS breach portal. This triggers HHS investigation.	CRITICAL
☐	**Notify HHS of Small Breaches (<500) Within 60 Days After Year-End**	Small breaches are logged and reported annually to HHS.	HIGH
☐	**Notify Affected Individuals Within 60 Days of Discovery**	Written notice with specific required content: breach description, PHI involved, steps taken.	CRITICAL
☐	**Notify Media if Breach Affects 500+ in a Single State**	Prominent media notice required alongside individual notification.	HIGH
☐	**Have a Pre-Approved Breach Notification Template Ready**	Do not draft notification language for the first time during an active incident.	HIGH
☐	**Engage Legal Counsel Before Any Breach Notification**	Notification language has legal consequences. Attorney review before sending.	HIGH
	Incident Response for PHI Incidents		
☐	**Document Your PHI Incident Response Plan**	Step-by-step plan for containment, assessment, notification, and recovery.	CRITICAL
☐	**Define First-Response Steps for Suspected PHI Breach**	Who to call, how to isolate, how to preserve evidence, within the first hour.	HIGH
☐	**Conduct Annual PHI Breach Simulation Exercise**	Tabletop exercise with leadership and legal. Test the plan before you need it.	HIGH
☐	**Maintain Forensic Capability to Investigate PHI Incidents**	Log retention, audit trails, and expertise to reconstruct what happened.	HIGH
☐	**Report PHI Security Incidents to CISO/Security Officer Within 1 Hour**	Internal escalation must be faster than external notification requirements.	HIGH
☐	**Conduct Post-Incident Review Within 72 Hours**	Root cause, timeline, gaps in controls, remediation plan — documented.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
	11 | THIRD-PARTY & VENDOR RISK MANAGEMENT		

✓	Checklist Item	What to Check / Notes	Priority
Vendor Assessment			
☐	**Conduct Security Assessment Before Sharing PHI with Any Vendor**	Security questionnaire, SOC 2 Type II review, or equivalent before onboarding.	CRITICAL
☐	**Classify All Vendors as PHI, Non-PHI, or Adjacent**	Every vendor in a risk tier. PHI vendors get highest scrutiny and BAA.	HIGH
☐	**Review Vendor SOC 2 Type II Reports Annually**	Not just at onboarding. Annual review catches control degradation.	HIGH
☐	**Assess Vendor Sub-Processor Chains**	Your vendor's vendors matter. Understand who else touches the PHI.	HIGH
☐	**Maintain a Vendor Risk Register with PHI Exposure Data**	Vendor name, PHI category, BAA status, last review, risk rating.	HIGH
☐	**Conduct On-Site or Virtual Security Reviews for Critical PHI Vendors**	Questionnaires alone are insufficient for high-risk vendors.	MEDIUM
Ongoing Vendor Governance			
☐	**Review All PHI Vendor BAAs Annually**	Business and data flows change. BAAs must reflect current reality.	HIGH
☐	**Monitor Vendor Security Incidents and Breaches**	Subscribe to vendor security advisories. Any vendor breach involving your PHI is your breach.	HIGH
☐	**Include Right-to-Audit Clause in All PHI Vendor Contracts**	You must be able to verify their controls when needed.	HIGH
☐	**Define Exit and PHI Return/Destruction Process for Each Vendor**	What happens to your PHI if you terminate the relationship?	HIGH
☐	**Reassess Vendor Risk on Major Contract Renewal**	Risk profile and controls may have changed since initial assessment.	MEDIUM
☐	**Track Vendor Incident Response Times Against BAA Requirements**	If a vendor fails to notify you in time, they're in violation — and so are you.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
12 | DATA RETENTION, BACKUP & SECURE DISPOSAL			
Retention Policies			
☐	**Define PHI Retention Periods for Each Data Category**	HIPAA does not set a single retention period — state law governs. Indian law adds complexity.	HIGH
☐	**Retain HIPAA Compliance Documentation for 6 Years**	Policies, procedures, risk analyses, training records, BAAs — all 6 years minimum.	CRITICAL
☐	**Align PHI Retention with US State Medical Record Laws**	State laws vary widely (5-10 years). Follow the most restrictive applicable law.	HIGH
☐	**Implement Automated Data Retention Enforcement**	Manual retention rarely works at scale. Automate deletion at retention expiry.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Document Legal Hold Process for PHI in Litigation**	When legal hold is triggered, automated deletion must be suspended for that data.	HIGH
☐	**Retain Audit Logs Separately from Application Data**	Logs have their own retention requirement. Do not delete them with operational data.	HIGH
	Backup Security		
☐	**Encrypt All PHI Backups at Rest**	Backup media is a common breach vector. Treat it as carefully as production data.	CRITICAL
☐	**Test PHI Backup Restores Monthly**	An untested backup may not restore. Know before you need it.	HIGH
☐	**Store Backups in Geographically Separate Locations**	Disaster recovery for healthcare data must survive regional events.	HIGH
☐	**Apply Access Controls to Backup Storage**	Backup systems are frequently overlooked in access reviews. Tighten them.	HIGH
☐	**Track Backup Media in Asset Inventory**	Tapes, drives, or cloud backup vaults — all tracked, inventoried, accounted for.	MEDIUM
	Secure Disposal		
☐	**Follow NIST SP 800-88 for Physical Media Disposal**	Degauss or physically destroy drives. Certificate of destruction required.	HIGH
☐	**Verify Cloud Storage Deletion Completeness**	Deleting a cloud object does not always delete all copies. Verify with provider.	HIGH
☐	**Destroy PHI in Paper Form with Cross-Cut Shredding**	Not standard office shredders. Cross-cut minimum, micro-cut preferred.	HIGH
☐	**Document Every PHI Disposal Event**	What was destroyed, when, how, by whom. Retain records for 6 years.	HIGH
☐	**Confirm Vendor PHI Deletion on Contract Termination**	Get written confirmation that PHI has been deleted/returned per BAA terms.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
	13 | TELEHEALTH & REMOTE CARE COMPLIANCE		
	Telehealth Platform Security		
☐	**Use Only HIPAA-Compliant Video Platforms for Telehealth**	Zoom for Healthcare, Doxy.me, Microsoft Teams Healthcare, or self-hosted equivalent with BAA.	CRITICAL
☐	**Execute BAA with Telehealth Video Platform Provider**	Consumer Zoom, Google Meet, and standard Teams are NOT HIPAA-compliant without BAA.	CRITICAL
☐	**Encrypt Telehealth Session Data End-to-End**	Video, audio, and chat must be encrypted. Verify provider encryption specifications.	CRITICAL
☐	**Implement Waiting Rooms for Patient Authentication**	Verify patient identity before admitting to session.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Prohibit Recording of Telehealth Sessions Without Consent**	If sessions are recorded, patient consent required and recordings are PHI.	HIGH
☐	**Ensure Chat/Messaging in Telehealth Platform Is Encrypted**	In-session messaging is PHI. Treat it accordingly.	HIGH
☐	**Disable Screen Capture During Telehealth Sessions Where Possible**	Technical controls against unauthorized screen capture.	MEDIUM
	Remote Work & Access Controls		
☐	**Enforce VPN for All Remote Access to PHI Systems**	Home networks are untrusted. VPN is mandatory for PHI access from outside office.	CRITICAL
☐	**Prohibit PHI Access from Personal/Unmanaged Devices**	MDM enrollment required before any device can access PHI.	HIGH
☐	**Train Remote Workers on HIPAA Physical Safeguards at Home**	Screen privacy, family members in workspace, clear desk policy for home offices.	HIGH
☐	**Prohibit Telehealth Consultations from Public Locations**	Clinician side: no PHI over public WiFi or in public spaces without privacy controls.	HIGH
☐	**Implement Split-Tunnel VPN Restrictions for PHI Traffic**	PHI-bound traffic must route through VPN even with split-tunnel configurations.	HIGH
☐	**Monitor Remote Access Sessions for Anomalies**	Unusual hours, unusual data volumes, unusual locations — alert and investigate.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
	14 | MOBILE HEALTH (mHEALTH) APP COMPLIANCE		
	Mobile App Security		
☐	**Encrypt PHI Stored Locally on Mobile Devices**	Any PHI cached on device must be encrypted using device hardware encryption.	CRITICAL
☐	**Implement Certificate Pinning for PHI API Communications**	Prevent MITM attacks on mobile PHI transmissions.	HIGH
☐	**Require App-Level PIN/Biometric Authentication**	Beyond device lock. App requires separate authentication before PHI access.	HIGH
☐	**Implement Remote Wipe of PHI from Lost Devices**	MDM capability to remotely wipe PHI if device is lost or stolen.	HIGH
☐	**Clear PHI from App Memory When Backgrounded**	PHI should not persist in app memory when app moves to background.	HIGH
☐	**Prohibit Screenshots of PHI Screens in App**	Technical controls on iOS (FLAG_SECURE on Android) to block screenshots.	HIGH
☐	**Conduct Mobile-Specific Penetration Testing**	Mobile attack surface differs from web. Separate testing required.	HIGH
	App Store & Distribution		

✓	Checklist Item	What to Check / Notes	Priority
☐	**Publish Accurate HIPAA Data Practices in App Store Privacy Labels**	App Store and Google Play require accurate privacy labels. PHI must be disclosed.	HIGH
☐	**Ensure Privacy Policy Covers HIPAA PHI Handling**	App privacy policy must describe PHI collection, use, and disclosure practices.	HIGH
☐	**Conduct Security Review Before Every Major App Release**	Security sign-off required before app update goes live.	HIGH
☐	**Implement App Attestation to Detect Rooted/Jailbroken Devices**	Block PHI access from compromised devices.	MEDIUM
☐	**Review Third-Party SDKs in App for PHI Leakage Risk**	Analytics SDKs, crash reporting, and ad SDKs can inadvertently capture PHI.	HIGH
☐	**Disable PHI Auto-Fill and Browser Autofill in App Forms**	Autofill systems can store PHI outside your control.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
15 | AI & MACHINE LEARNING WITH HEALTH DATA			
PHI in AI/ML Pipelines			
☐	**Obtain Appropriate Authorization Before Using PHI for AI Training**	Using PHI for model training requires authorization or proper de-identification.	CRITICAL
☐	**De-Identify PHI Before Using in AI Training Datasets**	HIPAA Safe Harbor or Expert Determination. Both have specific technical requirements.	CRITICAL
☐	**Execute BAA with Any AI Provider Processing Your PHI**	OpenAI, Anthropic, Google — only use HIPAA-BAA versions for PHI. Not standard APIs.	CRITICAL
☐	**Audit What PHI Goes Into AI Model Prompts**	PHI in prompts goes to provider's servers. Audit every call. Mask where possible.	CRITICAL
☐	**Document AI Model Training Data Provenance**	What patient data was used, when, under what authorization.	HIGH
☐	**Apply Access Controls to AI Training Datasets**	Training datasets with PHI must have the same access controls as production PHI.	HIGH
☐	**Scan AI Training Data for Unexpected PHI Before Use**	De-identification processes sometimes fail. Verify with automated scanning.	HIGH
AI Model Governance			
☐	**Document AI Model Decision-Making for Clinical Use Cases**	Explainability requirements for AI models used in clinical decision support.	HIGH
☐	**Validate AI Models for Bias Against Protected Patient Populations**	Healthcare AI bias can cause discriminatory outcomes. Test and document.	HIGH
☐	**Maintain Version History of AI Models Used in Clinical Decisions**	Know exactly which model version made which decisions and when.	HIGH
☐	**Implement Human Override for All AI Clinical Recommendations**	AI assists clinicians; it does not replace them. Override mechanism required.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Obtain Patient Consent Disclosure for AI-Assisted Care**	Patients should know when AI is involved in their care pathway.	MEDIUM
☐	**Monitor AI Models for Performance Degradation Over Time**	Model drift can cause unexpected PHI exposure or inaccurate clinical outputs.	MEDIUM

✓	Checklist Item	What to Check / Notes	Priority
16 | AUDIT, TESTING & CONTINUOUS COMPLIANCE			
Internal Audit Program			
☐	**Conduct Annual Internal HIPAA Compliance Audit**	Formal audit against all HIPAA rule requirements. Document findings and remediation.	CRITICAL
☐	**Conduct Quarterly Technical Security Reviews**	Penetration testing, vulnerability scanning, configuration review.	HIGH
☐	**Audit All PHI System Access Logs Monthly**	Automated + manual review for unauthorized or unusual access patterns.	HIGH
☐	**Conduct Surprise Audits of Physical Safeguards**	Physical controls degrade. Unannounced checks keep them honest.	MEDIUM
☐	**Audit Third-Party BAA Compliance Annually**	Verify sub-BAs are meeting their obligations, not just that they signed.	HIGH
☐	**Track Audit Findings to Closure in a Remediation Register**	Every finding: owner, severity, due date, status. Review weekly.	HIGH
External Assessment & Penetration Testing			
☐	**Conduct Annual Third-Party HIPAA Security Assessment**	External assessors provide unbiased view of your compliance posture.	HIGH
☐	**Conduct Annual External Penetration Testing of PHI Systems**	HIPAA doesn't mandate pen testing, but OCR expects reasonable testing.	HIGH
☐	**Include Social Engineering Tests in Annual Security Assessment**	Phishing simulations targeting PHI access are a key attack vector.	HIGH
☐	**Test Physical Security Controls as Part of Annual Assessment**	Tailgating, badge cloning, unauthorized entry attempts.	MEDIUM
☐	**Remediate Penetration Testing Findings Within Defined SLAs**	CRITICAL: 24 hr. HIGH: 30 days. MEDIUM: 90 days. Document all.	HIGH
☐	**Share Pen Test Results with Covered Entity Clients on Request**	Some CE clients contractually require sight of your security test results.	MEDIUM
Continuous Monitoring			
☐	**Implement SIEM for Real-Time PHI System Monitoring**	Centralized log analysis with HIPAA-specific correlation rules.	HIGH
☐	**Deploy Intrusion Detection Systems on PHI Network Segments**	Alert on suspicious traffic patterns within PHI network segments.	HIGH
☐	**Monitor for Unauthorized PHI Exports and Downloads**	Bulk download alerts, after-hours access alerts, unusual query patterns.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
☐	**Conduct Vulnerability Scanning of PHI Systems Weekly**	Authenticated scans. New vulnerabilities appear constantly.	HIGH
☐	**Alert on Any New Public Exposure of PHI Systems**	Continuous ASM scanning. Any new public-facing PHI endpoint triggers alert.	HIGH

✓	Checklist Item	What to Check / Notes	Priority
17 | DOCUMENTATION, POLICY & GOVERNANCE			
Required HIPAA Policies			
☐	**Privacy Policy (HIPAA Privacy Rule Requirements)**	Permitted uses, patient rights, minimum necessary, complaint procedures.	CRITICAL
☐	**Security Policy (HIPAA Security Rule Requirements)**	Administrative, physical, and technical safeguard requirements.	CRITICAL
☐	**Breach Notification Policy**	Detection, assessment, internal escalation, notification procedures and timelines.	CRITICAL
☐	**Workforce Training and Sanctions Policy**	Training requirements, sanction levels, documentation and enforcement.	HIGH
☐	**Access Control and Password Policy**	Password complexity, MFA requirements, access provisioning and revocation.	HIGH
☐	**Device and Media Control Policy**	Approved devices, encryption requirements, disposal procedures.	HIGH
☐	**Incident Response Policy**	PHI incident classification, response steps, team roles, documentation.	HIGH
☐	**Third-Party and Vendor Management Policy**	BA identification, BAA requirements, vendor risk assessment process.	HIGH
☐	**Data Retention and Destruction Policy**	Retention periods, destruction methods, documentation requirements.	HIGH
☐	**Remote Work and Telehealth Security Policy**	Device requirements, VPN requirements, physical safeguard expectations.	HIGH
Policy Management			
☐	**Review and Update All HIPAA Policies Annually**	Policies must reflect current operations and regulatory changes.	CRITICAL
☐	**Get Legal Review of All HIPAA Policies Before Publication**	HIPAA compliance language has legal implications. Attorney review required.	HIGH
☐	**Distribute Policies to All Workforce and Require Acknowledgment**	Written acknowledgment on policy distribution. Retained for 6 years.	HIGH
☐	**Version-Control All HIPAA Compliance Documents**	Know what policy was in effect at any given date. Important for breach investigations.	HIGH
☐	**Store All HIPAA Documentation for Minimum 6 Years**	Policies, risk analyses, training records, BAAs, audit reports — all 6 years.	CRITICAL

✓	Checklist Item	What to Check / Notes	Priority
☐	**Make Policies Accessible to All Workforce Members**	Policies locked in a compliance folder no one can access defeats the purpose.	MEDIUM
Leadership & Governance			
☐	**Present HIPAA Compliance Status to Leadership Quarterly**	Board/leadership visibility on compliance posture, findings, and risk.	HIGH
☐	**Allocate Dedicated Budget for HIPAA Compliance Activities**	Underfunded compliance programs fail. Budget line item, not ad-hoc spend.	HIGH
☐	**Designate Executive Sponsor for HIPAA Program**	Leadership accountability beyond the Privacy and Security Officers.	MEDIUM
☐	**Include HIPAA Risks in Enterprise Risk Register**	HIPAA non-compliance is a business risk. It belongs in the risk register.	HIGH
☐	**Define HIPAA KPIs and Track Them Monthly**	Training completion rate, open findings count, breach response time, audit score.	MEDIUM
☐	**Subscribe to HHS OCR Guidance and HIPAA Updates**	HHS regularly releases new guidance. Stay current with regulatory changes.	MEDIUM

This checklist references HIPAA Privacy Rule (45 CFR Part 164, Subparts A & E), Security Rule (Subparts A & C), Breach Notification Rule (Subpart D), HHS OCR guidance, NIST SP 800-66r2 (HIPAA Security Rule implementation guidance), India DPDP Act 2023, and IT Act 2000 as of February 2026. Regulatory requirements evolve — review this document at least annually.

For HIPAA compliance audits, security assessments, or cloud infrastructure implementation: **sales@bithost.in | +91 911-336-6525**