SAIGON TECHNOLOGY
YOUR SUCCESS IS OUR MISSION

AI-Driven Software Development

HIPAA COMPLIANCE CHECKLIST

A Practical Verification Framework for Healthcare Engineering & Product Teams

Thanh (Bruce) Pham, CEO, Saigon Technology

April 2026

A practical HIPAA compliance framework for engineering teams building secure healthcare applications, telehealth platforms, and AI-powered digital health solutions.

Table of Contents

Sections

Executive Summary

Healthcare data breaches reached record highs in 2024, exposing more than 168 million patient records. For healthcare organizations and digital health startups, building a HIPAA-compliant app is no longer optional. The good news is that compliance is a solvable engineering problem when teams plan for it from day one.

This checklist consolidates 100+ verification items across 12 sections. It maps HIPAA's Security Rule (Administrative, Technical, and Physical Safeguards) to the practical engineering, vendor, and operational decisions a development team makes during a real healthcare project.

Built for engineering and product teams

This checklist is designed for CTOs, engineering leads, product managers, and DevOps teams building healthcare applications that handle Protected Health Information (PHI). Use it as a living document during architecture reviews, sprint planning, vendor evaluations, and pre-launch readiness checks.

When to use each section

Phase	Sections to apply
Architecture Review	Sections 1, 3, 5, and 8 validate technical and cloud decisions before any code is written.
Build Phase	Sections 3 and 6 anchor the engineering and vendor work. Run them as living tickets in your sprint board.
Pre-Launch	Sections 7 and 9 are the gating criteria. Production traffic does not begin until both are checked.
Post-Launch	Section 7 plus Section 10 form the basis of an ongoing compliance program. Run quarterly.

> **KEY PRINCIPLE**
>
> HIPAA compliance is a continuous program, not a launch event. Most enforcement actions target organizations with compliant launches but no maintenance program after go-live. Plan for that reality from the architecture phase.

Section 1, Reference Architecture for HIPAA Apps

A typical HIPAA-compliant healthcare platform has six core layers. Each layer carries specific compliance requirements. Use this reference architecture as a starting point when designing a new healthcare application or auditing an existing one.

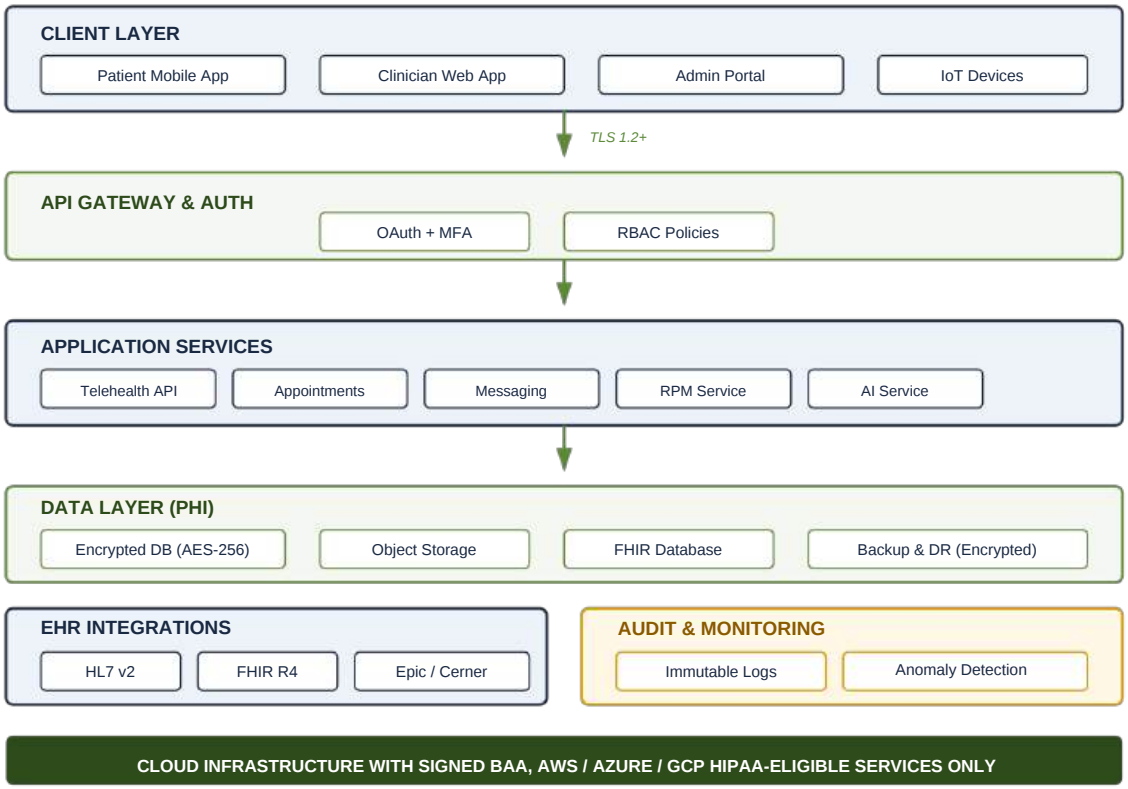

Figure 1, Reference architecture for a HIPAA-compliant healthcare platform with telehealth, EHR integration, and AI services.

How to read this diagram

Every layer connects to the BAA-covered cloud infrastructure at the bottom. Encryption flows from the client (TLS 1.2+) through the API gateway, into the application services, and lands in the encrypted data layer. Audit and monitoring observe every PHI access event across all layers. EHR integrations use HL7 or FHIR over TLS, never plain HTTP.

Section 2, Administrative Safeguards

The policies and procedures around your engineering work. Engineering teams often skip these because they are not shippable code. Administrative safeguard gaps remain one of the most common HIPAA audit findings.

CRITICAL BEFORE GO-LIVE

- [ ] **Risk Analysis.** PHI threats documented for every new feature touching patient data.
- [ ] **Risk Assessment.** Likelihood and impact rated for each identified threat.
- [ ] **Security Officer Assigned.** A named, accountable individual with HIPAA security responsibility.
- [ ] **Incident Response Plan.** Named owners and escalation paths assigned.
- [ ] **Breach Response Plan.** 60-day notification workflow documented and rehearsed.

RECOMMENDED

- [ ] **Workforce Training.** All staff have completed HIPAA policy training within the last 12 months.
- [ ] **Information Access Management.** Access policies documented per role.
- [ ] **Sanction Policy.** Disciplinary procedures for workforce HIPAA violations documented.
- [ ] **Minimum Necessary Standard.** PHI access limited to what each role requires.

ONGOING COMPLIANCE

- [ ] **Annual Risk Re-Assessment.** Reviewed and updated as the application evolves.
- [ ] **BAA Inventory Review.** Quarterly confirmation that every PHI-touching vendor still has a valid BAA.

Section 3, Technical Safeguards

The controls your engineering team builds into the application. This is where most of the day-to-day work lives. Group your verification by Authentication, Encryption, and Monitoring.

CRITICAL, AUTHENTICATION

- [ ] **Unique User Identification.** Every account has a unique ID. No shared logins, ever.
- [ ] **Role-Based Access Control (RBAC).** Least-privilege enforced by job function.
- [ ] **Multi-Factor Authentication.** Enabled for all admin and clinical roles.
- [ ] **Automatic Logoff.** Session timeout configured on web and mobile.

CRITICAL, ENCRYPTION

- [ ] **Encryption at Rest.** AES-256 or stronger for all databases, file storage, and backups.
- [ ] **Encryption in Transit.** TLS 1.2+ for all network communication, including internal service calls.
- [ ] **Mobile Device Encryption.** All cached PHI encrypted on user devices.
- [ ] **Secrets Management.** No hardcoded tokens, API keys, or credentials in code.

RECOMMENDED, MONITORING

- [ ] **Audit Controls.** Every read, write, and configuration change to PHI captured.
- [ ] **Immutable Audit Logs.** Logs are append-only and cannot be altered after the fact.
- [ ] **Data Integrity Controls.** Unauthorized PHI modification detection active.
- [ ] **Log Redaction.** PHI not leaking into application logs or third-party error trackers.
- [ ] **Emergency Access Procedure.** Break-glass access defined, logged, and tested.

Section 4, Physical Safeguards & Mobile Security

For cloud-native apps, hosting providers cover most of the physical layer. Mobile devices are where engineering teams actually focus. Lost or stolen devices are the second most common cause of reportable breaches behind hacking.

Physical Safeguards (cloud-managed)

- [ ] **Device Controls.** Workstation and mobile access policies documented.
- [ ] **Data Backup & Recovery.** Tested restore procedures in place.
- [ ] **Emergency Access Procedures.** Critical clinical scenario protocols ready.
- [ ] **Device Disposal.** PHI wiped before any device decommissioning.

Mobile Security (engineering-owned)

- [ ] **Device-Level Encryption.** All PHI on devices encrypted, including cached data.
- [ ] **Jailbreak / Root Detection.** Enforced at app launch.
- [ ] **Automatic Logoff on Mobile.** Inactivity timeout configured.
- [ ] **Secure Local Storage.** No PHI in plain-text caches, SharedPreferences, or UserDefaults.
- [ ] **Biometric Fallback Security.** Weak fallback paths blocked.
- [ ] **Remote Wipe Capability.** Lost or stolen device procedure defined.
- [ ] **Push Notification Hygiene.** No PHI in notification body. Use generic alerts ("New message from Dr. Smith").

> **MOST COMMON MOBILE FAILURE**
>
> PHI rendered in push notification preview text. Patient sees "Lab result: HIV positive" on a locked phone in public. This single oversight has triggered multiple OCR settlements. Use generic notification copy and require app open to view details.

Section 5, Cloud Infrastructure

Major cloud providers offer HIPAA-eligible services. Three things still belong to your team: a signed BAA, eligible services only, and correct configuration. Misconfiguration is the most common breach cause on cloud-hosted healthcare platforms.

CRITICAL BEFORE GO-LIVE

- [ ] **BAA Signed with Cloud Provider** before any production PHI traffic.
- [ ] **HIPAA-Eligible Services Only.** Every service verified against the provider's official eligible list.
- [ ] **Shared Responsibility Model** reviewed and documented.
- [ ] **PHI Data Flows** documented across all cloud services.

AWS specifics

- [ ] **AWS CloudTrail.** Audit logging active across all regions.
- [ ] **Amazon S3 Encryption.** Server-side encryption on all buckets.
- [ ] **Amazon RDS Encryption.** Database encryption at rest enabled.
- [ ] **Lambda PHI Handling.** Reviewed per function. No PHI in CloudWatch logs.

Azure & Google Cloud specifics

- [ ] **Azure Health Data Services.** FHIR workloads using compliant services.
- [ ] **Google Cloud Healthcare API.** FHIR-compliant APIs configured for EHR exchange.
- [ ] **Cloud Audit Logs.** Admin, data access, and system event logs active.

Section 6, Vendor & BAA Management

Every vendor that touches PHI needs a signed Business Associate Agreement. Missing BAAs with downstream subprocessors are a leading source of compliance findings.

COMMONLY MISSED BAAS

- [ ] **Push Notification Service.** If notifications can include PHI.
- [ ] **Email and SMS Gateway.** Appointment reminders and clinical alerts.
- [ ] **Error Tracking Platform.** Sentry, Datadog, or equivalent.
- [ ] **Analytics & Session Recording.** Mixpanel, Amplitude, FullStory, Hotjar.
- [ ] **Customer Support System.** Help desk and ticketing tools.
- [ ] **AI Vendor.** Any AI tool processing PHI, including OpenAI Enterprise, Anthropic, or self-hosted models with vendor support.
- [ ] **Third-Party APIs.** Any API receiving or returning PHI.

CRITICAL BEFORE GO-LIVE

- [ ] **Cloud Provider BAA** signed before production traffic begins.
- [ ] **Permitted Uses and Disclosures** defined and scoped in every BAA.
- [ ] **Breach Notification Obligations.** Vendor timelines specified.
- [ ] **Data Modification and Deletion.** PHI destruction on offboarding documented.

ONGOING COMPLIANCE

- [ ] **Quarterly Vendor Reviews** scheduled and tracked.
- [ ] **Recognized Security Practices.** HITECH RFI documentation maintained.

Section 7, Audit Logging & Incident Response

HIPAA's 60-day breach notification window starts from discovery, not confirmation. Engineering teams need both observability tooling and a documented response playbook ready before go-live.

Audit Logging

- [ ] **Infrastructure Logging** active across all cloud services.
- [ ] **Application-Level PHI Logging.** Read, write, and delete events captured.
- [ ] **Immutable Logs.** Append-only, tamper-proof log storage.
- [ ] **Log Retention Policy** defined and enforced (typically 6 years).
- [ ] **Log Access Controls.** Audit logs protected from unauthorized access.

Ongoing Monitoring

- [ ] **Real-Time Anomaly Detection.** Suspicious access patterns flagged automatically.
- [ ] **Audit Log Review Schedule.** Documented cadence with named owner.
- [ ] **Workforce Training Refresh.** New staff onboarding process covered.

Incident Response

- [ ] **Incident Response Plan** documented with named owners and escalation paths.
- [ ] **60-Day Notification Window.** Discovery-to-report timeline mapped.
- [ ] **Pre-Approved Breach Templates** stored and accessible.
- [ ] **OCR Reporting Procedure** for breaches affecting 500+ individuals.
- [ ] **Annual Breach Simulation.** Tabletop exercise completed.

COMMON LOGGING MISTAKE

Application logs that include request bodies leak PHI into your error tracker. Configure log redaction at the framework level (request middleware, structured logger filters) so PHI is stripped before it reaches Sentry, Datadog, or CloudWatch.

Section 8, HIPAA Risks in AI Applications

AI features in healthcare apps (medical summarization, clinical chatbots, voice transcription) introduce new HIPAA risks. Most existing checklists miss them entirely.

CRITICAL AI CONTROLS

- ☐ **Do not train AI models using PHI.** Vendor terms must explicitly prohibit using your PHI for model training.
  Enterprise AI platforms may support HIPAA-aligned deployments when properly configured.
- ☐ **BAA in Place with AI Vendor.** No exceptions. Even prototype features need this before touching real PHI.
- ☐ **PHI Redaction Before AI Processing.** Strip identifiers (name, MRN, DOB) before sending data to LLMs when possible.
- ☐ **AI Prompts and Outputs Logged.** Full audit trail of what was sent and what came back.
- ☐ **Human Review Required** for high-risk clinical AI outputs (treatment recommendations, diagnostic suggestions).

REAL IMPLEMENTATION EXAMPLE, AI NOTE-TAKING

A clinician records a 30-minute patient visit. The mobile app uploads the audio to a HIPAA-eligible speech-to-text service (under BAA). The transcript is then summarized by an LLM with a no-training agreement. Both the audio file and the transcript are stored encrypted in the FHIR-linked patient record. Every step (upload, transcription, summarization, storage) writes to the audit log with user ID, timestamp, and patient context. The clinician reviews and edits the AI summary before it is committed to the EHR. **The AI is an assistant, not the source of record.**

HIGH RISK, AI CHATBOTS HANDLING PHI

Patient-facing AI chatbots that answer health questions are a fast-growing breach vector. If the chatbot can access PHI, every conversation is a HIPAA event. Log it, scope it, and route through a BAA-covered model. Never use a consumer API like the public ChatGPT endpoint for these flows.

Section 9, Pre-Launch Validation

Final security and compliance validation before production. No production PHI traffic until every box below is checked.

Security Testing

- ☐ **External Penetration Testing** completed by a third-party security firm.
- ☐ **Vulnerability Scanning** run on all infrastructure components.
- ☐ **Static Code Analysis.** Automated scanning on every pull request.
- ☐ **Dynamic Code Analysis.** Runtime security test suite complete.
- ☐ **Dependency Scanning.** Third-party libraries checked for known CVEs.
- ☐ **Mobile Testing** run on real physical devices, not simulators only.

Compliance Validation

- ☐ **HIPAA Safeguard Review.** Every administrative, technical, and physical requirement verified.
- ☐ **Vendor BAAs Verified.** All production-stack vendors confirmed.
- ☐ **Encryption Paths Reviewed.** No unencrypted PHI paths in production.
- ☐ **Logging Leakage Audit.** PHI not leaking into non-eligible endpoints.
- ☐ **RBAC Role Review.** Dev-wide admin roles tightened before launch.
- ☐ **Final Security Sign-Off.** Security lead and compliance officer approval.

Section 10, What Most Healthcare Startups Miss

Eight failure patterns we see repeatedly when reviewing healthcare apps. Verify your team avoids each one before go-live.

01 **Treating HIPAA as a launch checklist**
No ongoing program after go-live. Compliance requires annual risk assessments and quarterly BAA reviews to stay defensible.

02 **Missing BAAs with downstream subprocessors**
Push notifications, error tracking, and analytics tools often slip through vendor reviews. Each one is a business associate if PHI passes through.

03 **PHI stored in non-eligible cloud services**
Logs, CDN cache, and archive tiers using non-eligible services create silent exposure that audits will surface.

04 **Hardcoded tokens and broad admin roles**
Dev-wide admin roles never tightened before launch are a top finding in compliance reviews.

05 **Mobile safeguard failures**
No automatic logoff, insecure local storage, weak biometric fallback, PHI in push notification previews.

06 **Ignoring breach notification timing**
The 60-day window starts from discovery, not confirmation. Delayed reporting compounds penalties.

07 **AI features without PHI guardrails**
Model inputs or outputs that expose PHI without redaction, BAA, or audit trail. Patient-facing chatbots are a particular risk.

08 **IoT and wearable data handling gaps**
Device-level PHI outside encryption and access control scope is a growing source of regulator attention.

Section 11, Recommended HIPAA-Ready Stack

Engineering teams ask us this constantly. Below is a starting reference stack we use on healthcare projects. Specific choices vary by team and use case, but every option listed here is BAA-eligible and field-tested.

CLOUD PLATFORM

AWS with HIPAA-eligible services (EC2, RDS, S3, Lambda, CloudTrail).
Azure with Azure Health Data Services for FHIR.
GCP with Cloud Healthcare API.

EHR INTEROPERABILITY

HL7 v2 for legacy integrations.
FHIR R4 for modern API exchange.
SMART on FHIR for app-launch scenarios.

AUTHENTICATION & IDENTITY

Auth0, **AWS Cognito**, **Azure AD B2C**. OAuth 2.0 + OIDC. MFA mandatory for clinical roles.

AUDIT LOGGING

AWS CloudTrail + structured app logs to S3 with object-lock for immutability.
Azure Monitor with retention policies.

ENCRYPTION

AES-256 at rest, **TLS 1.2+** in transit.
Key management via AWS KMS, Azure Key Vault, or GCP KMS.

MONITORING & OBSERVABILITY

Datadog or **New Relic** with BAA.
AWS GuardDuty or **Azure Defender** for anomaly detection.

TELEHEALTH & REAL-TIME

Agora, **Twilio Video**, or **Wowza** with a HIPAA-supporting configuration.

WebRTC with TURN servers under BAA.

AI & ML

OpenAI Enterprise, **Anthropic Claude for Work**, or **Azure OpenAI**.

No-training clauses. BAA where applicable.

> **NOTE**
>
> A BAA-eligible service alone does not make your app compliant. Configuration, vendor scope, and ongoing monitoring still belong to your team.

About Saigon Technology & Next Steps

Successful HIPAA compliance requires more than encryption. It requires compliant infrastructure, BAA-covered vendors, and healthcare domain expertise at every layer of your stack.

After completing this checklist

- Review every unchecked item with your security and engineering leads.
- Prioritize Technical Safeguards and BAA gaps as P1 before launch.
- Schedule annual risk assessment and quarterly BAA review cadence.
- Engage an external security firm for penetration testing.
- Budget ongoing compliance operations beyond the build phase.

Trusted by healthcare startups and providers

14+	800+	300+	400+
Years in software development	Projects delivered across web and mobile platforms	Clients across the US, EU, Australia, and Singapore	Engineers across Vietnam development centers

Saigon Technology partners with healthcare startups, hospitals, and healthcare providers on telehealth platforms, EHR/EMR integration, remote patient monitoring, patient engagement portals, and AI-powered healthcare applications.

Our teams support healthcare projects with HIPAA-ready development processes, secure cloud infrastructure, post-launch support, and experience working with US healthcare compliance requirements.

Talk to our healthcare engineering team: https://saigontechnology.com/contact/

Read more case studies: https://saigontechnology.com/case-studies/