US EDITION · 2026

# The HIPAA-Ready Healthcare Software Buyer's Kit

A plain-English guide for founders, product leads and clinical operators who are about to buy, build or replace a healthcare software product in the United States. Written by the engineers who actually ship these systems, not by a marketing team.

Prepared for you

## What is inside this kit

- A 60-question vendor and internal build checklist you can run in one afternoon
- Realistic 2026 US cost and timeline ranges for the five most common healthcare builds
- A Business Associate Agreement readiness worksheet, in language your legal team will accept
- The full US compliance stack reference: HIPAA, HITECH, ONC, CMS Interoperability, SOC 2 and the state laws that actually apply
- The mistakes we see US healthcare startups make in year one, and what to do instead

*Prepared for: the person on your team who has to sign off on the vendor, the compliance stack and the go-live date. If that is you, keep reading. If it is not, forward this to them.*

# A short note before you start

We wrote this kit because most of the healthcare buyer guides floating around the internet are, frankly, filler. They repeat the same five bullet points about HIPAA, mention encryption at rest as if it is a differentiator, and then quietly try to sell you their platform.

This one is different. It is the same internal document our team reaches for when a US clinic, digital health startup or hospital innovation group asks us to scope a build. Nothing here is theoretical. Every checklist item, every price band, every warning has come out of a real project we have shipped or rescued.

Read it end to end once. Then keep it open in a tab while you talk to vendors. If a vendor cannot answer the questions on page 4 in plain language, you already have your answer.

## Who this is for

- Founders shipping their first healthcare product in the US market
- Product managers replacing a legacy EHR, RCM or patient portal system
- Clinical operators evaluating a telemedicine or ambient scribe vendor
- Compliance leads who need a common language with their engineering team
- Investors doing technical diligence on a health-tech deal

## How to use it

Sections one through three are for the person making the buy or build decision. Sections four and five are for the person implementing it. Sections six and seven are for whoever has to defend the choice to a board, an auditor or a hospital CIO.

If you only have twenty minutes, read the checklist on page 4, the cost tables on page 6, and the red flags on page 10. That covers the ninety percent case.

# 1. The 60-question vendor and build checklist

Print this. Sit with it. Ask a vendor to answer in writing, or ask your own team to score each item honestly. A yes needs evidence, not a nod. A no is not a deal-breaker, but three or more in the same section usually is.

## Legal and compliance posture (10)

- Will the vendor sign a Business Associate Agreement without carve-outs on breach notification
- Do they name a specific person accountable for HIPAA compliance, not a generic role
- Can they show a current SOC 2 Type II report, not just a Type I
- Do they carry cyber liability insurance of at least five million US dollars
- Have they had a reportable breach in the last 36 months, and if so, what changed
- Do they support Right of Access requests within the 30 day HIPAA window
- Do they log every PHI access event, and can you export those logs
- Do they have a written incident response plan you can read
- Do they support your state laws on top of HIPAA, in writing
- Who owns the data if the contract ends, and how is it returned or destroyed

## Architecture and hosting (10)

- Is production data hosted in a US region, and can they prove data residency
- Do they use dedicated tenancy or shared multi-tenant, and how is PHI isolated
- Is all PHI encrypted at rest with AES-256 and in transit with TLS 1.2 or higher
- Are encryption keys managed in a customer-controlled KMS, or vendor-controlled
- Do backups include PHI, and are they encrypted the same way as production
- What is the documented Recovery Time Objective and Recovery Point Objective
- Is there a working disaster recovery test on record from the last 12 months
- Do they run in a region with a signed cloud BAA (AWS, Azure or Google Cloud)
- How is production access controlled: SSO, MFA, session recording, break-glass
- Can they hand over an infrastructure architecture diagram without redacting the important parts

## Product and clinical workflow (10)

- Does the product match the actual workflow of your clinicians, or does it force a new one

- How long does it take to onboard a new clinician to full productivity
- Can non-technical staff configure forms, templates and workflows without a code release
- Does the product handle the state-specific consent flows for your service line
- Is there a real accessibility posture (WCAG 2.1 AA), tested, not claimed
- Are patient-facing screens available in Spanish at a clinical reading level
- Does the product support asynchronous care, or only synchronous
- How does the product behave when the internet drops mid-visit
- Can a clinician correct or amend a note after signing, with a proper audit trail
- Is there a real, staffed help desk clinicians can call at 8pm on a Tuesday

## Interoperability (10)

- Does the product speak FHIR R4 natively, or through a translation layer
- Which specific HL7 v2 message types are supported for lab, ADT and orders
- Is there a live integration with Epic and Cerner in production today, not on the roadmap
- Does it support SMART on FHIR launch for embedded apps
- Can it push and pull from a state Health Information Exchange
- Is the product certified under the ONC Health IT Certification Program, and for which criteria
- Does it meet CMS Interoperability and Patient Access rule requirements
- Are lab result codes mapped to LOINC, and medications to RxNorm
- Does it support the USCDI v3 data classes your workflow needs
- How does it handle patient matching across sources without creating duplicate records

## Billing, payments and RCM (10)

- Does it generate clean 837P and 837I claims, or only rely on a clearinghouse
- Can it consume 835 remittance files and post payments automatically
- Does it support real-time eligibility checks through a 270 or 271 transaction
- Is there prior authorization support, and for which payers
- How does it handle patient responsibility estimates before the visit
- Does it support HSA, FSA and card on file with a PCI-compliant vault
- Is there a working denial management workflow, or just a report
- Can it handle sliding scale, capitated and value-based arrangements
- Does it integrate with your practice management or general ledger without custom ETL
- What is the average first-pass claim acceptance rate across their US customer base

## Commercial and total cost of ownership (10)

- Is the pricing per provider, per patient, per encounter or per module, and does it change at scale
- What is the total three-year cost with realistic patient volume, not the sales quote
- Are integrations, custom reports and additional environments in the base price
- Is there an implementation fee, and does it cap or run on time and materials
- What is the contractual notice period, and can you exit for cause without penalty
- Are price increases contractually capped, and to what
- Who pays for annual security assessments and penetration tests
- Are you charged for data export at the end of the contract
- Is there a real reference customer of your size and specialty you can speak to
- Would you sign this contract if you had to write the check personally

UZ TECHNOLOGIES
uztechnologies.co.in · Prepared for you

# 2. Real 2026 US cost and timeline ranges

These are the bands we quote when a US client walks in with a clean brief. Anything meaningfully below the low end usually skips compliance, testing or the audit trail. Anything above the high end usually has scope that could be phased. Ranges assume a US-facing product, HIPAA in scope, one integration with an EHR or clearinghouse and a real go-live, not a demo.

## Cost bands, US market, 2026

| Build type | Realistic range (USD) |
|---|---|
| MVP telemedicine platform (web plus one mobile OS) | 85,000 to 160,000 |
| Full telemedicine platform (web, iOS, Android, admin) | 180,000 to 340,000 |
| Patient portal on top of an existing EHR | 60,000 to 140,000 |
| EHR or FHIR integration layer, single source system | 45,000 to 110,000 |
| EHR or FHIR integration layer, multi-source | 120,000 to 260,000 |
| Ambient AI clinical documentation, MVP | 140,000 to 260,000 |
| Revenue cycle management workflow module | 90,000 to 220,000 |
| HIPAA-aligned custom mobile app, single platform | 55,000 to 130,000 |
| SOC 2 Type I readiness, from a clean baseline | 22,000 to 55,000 plus auditor fee |
| Annual maintenance, security patching and on-call | 18 to 26 percent of build cost per year |

## Timeline bands

| Milestone | Typical duration |
|---|---|

UZ TECHNOLOGIES
Prepared for you
uztechnologies.co.in

| | |
|---|---|
| Discovery, clinical workflow mapping and compliance scoping | 3 to 6 weeks |
| Design, prototyping and clinical validation | 4 to 8 weeks |
| Core build and internal QA | 10 to 20 weeks |
| Security hardening and penetration test | 3 to 5 weeks |
| Pilot with one clinic or provider group | 4 to 8 weeks |
| General availability launch | 2 to 4 weeks |

### A note on the low end

If a vendor quotes you well below the low end of these bands, ask two questions in writing. First: is a Business Associate Agreement included and signed by go-live. Second: does the price include a third-party penetration test before launch. If either answer is no, the quote is not comparable. You are not buying the same product.

UZ TECHNOLOGIES
uztechnologies.co.in · Prepared for

# 3. The Business Associate Agreement readiness worksheet

Most BAA delays are caused by the same three or four points. Walk through this worksheet with your vendor before you send anything to legal. It will save you a fortnight.

### Breach notification window

HIPAA requires notification without unreasonable delay and no later than 60 days. Do not accept language that stretches this. Ask for 30 to 45 days in writing.

### Subcontractor flow-down

The vendor must contractually bind their subcontractors (cloud, email, SMS, analytics) to the same BAA terms. Ask for the list of subcontractors that touch PHI.

### Right of access

Patients can request their records within 30 days. Confirm the vendor supports this workflow, not just the export.

### Data return or destruction

On contract termination, PHI must be returned or destroyed within a defined window. Get the window in the BAA, not in a side letter.

### Minimum necessary standard

The vendor should only access PHI that is required for the service. Ask how they enforce this technically, not just in policy.

### Audit rights

You should have the right to audit the vendor's HIPAA controls, either directly or through a SOC 2 report.

### Indemnity and liability

Do not accept a total liability cap equal to twelve months of fees. Healthcare breaches cost far more.

### State law overlays

If you operate in California, Texas, New York, Illinois or Massachusetts, name the state laws in the BAA. Do not leave it implied.

### Governing law

Prefer a US state you operate in, not the vendor's home state.

UZ TECHNOLOGIES
uztechnologies.co.in
Prepared for you

# 4. The US healthcare compliance stack, in one place

You have probably seen this list scattered across ten different vendor decks. Here it is in one reference page, with the version that actually applies in 2026 and a plain-English note on what each one means for your product.

### HIPAA Privacy Rule

Governs how PHI can be used and disclosed. Applies to covered entities and their business associates. This is the baseline, not the ceiling.

### HIPAA Security Rule

Requires administrative, physical and technical safeguards. Read the technical safeguards section before you talk architecture.

### HITECH Act

Extends HIPAA with breach notification rules and higher penalties. Also created the incentives that funded the EHR rollout you are now integrating with.

### HIPAA Omnibus Rule (2013)

Made business associates directly liable and tightened breach notification. Yes, it still applies.

### ONC Health IT Certification Program

If you touch certified EHR functionality or claim USCDI compliance, this is your reference.

### 21st Century Cures Act, information blocking rule

You cannot design a product that unreasonably blocks the exchange of electronic health information. Applies more broadly than most teams think.

### CMS Interoperability and Patient Access rule

Requires payer APIs and patient access. If your product touches Medicare Advantage, Medicaid or ACA plans, this affects you.

### USCDI v3

The set of data classes that must be exchangeable. Map your data model to it early, not late.

### FHIR R4 and US Core

The interoperability standard. If you are building anything that touches an EHR after 2024 without FHIR, you are building tech debt.

### SOC 2 Type II

Not a HIPAA requirement, but every serious US buyer will ask for it. Plan Type I for launch, Type II by month 15.

### HITRUST CSF

Optional but valuable if you sell to health systems and payers. Expensive. Do not start here.

### State privacy laws

California CMIA and CPRA, Texas HB300, New York SHIELD, Illinois BIPA if you do any biometric work, Massachusetts 201 CMR 17, Washington My Health My Data. Read the ones that apply.

### PCI DSS

If you take card payments, even through a hosted vault, you have a scope to manage. Do not skip it.

### ADA and Section 508

Accessibility is a legal exposure, not a nice to have. Design for WCAG 2.1 AA from day one.

UZ TECHNOLOGIES
uztechnologies.co.in · Prepared for you

# 5. The mistakes we see US healthcare teams make

None of these are theoretical. Each one has cost a team we know real money, real time, or a customer they wanted to keep.

## Treating HIPAA as a checkbox at the end

Compliance is cheapest when it is designed in. Retrofitting an application to be HIPAA-safe after launch typically costs three to five times what building it right would have cost, and it never gets to the same place.

## Confusing a hosting BAA with a compliant product

AWS, Azure and Google Cloud all offer BAAs. Signing one does not make your application HIPAA-safe. It only removes one class of risk from the hosting layer. Your code and configuration still have to do the work.

## Skipping the third-party penetration test

An internal QA pass is not a security test. A real US buyer will ask for a recent third-party penetration test. Budget it. Book it before launch, not after.

## Building a portal patients do not use

US patients are tired of portals that only work well on desktop, require a password reset every login, and hide the one thing they actually came for. If the first-visit success rate on mobile is not above 80 percent, the product is not done.

## Under-scoping integration work

EHR and clearinghouse integrations are almost always the pole in the tent. Assume the vendor timeline for the integration is optimistic, and plan a buffer.

## Ignoring state law overlays

California, Texas, New York, Illinois, Massachusetts and Washington all have overlays that go beyond HIPAA. If you serve those states, read the laws.

## Choosing a stack that no US engineer wants to touch

Healthcare products live for a decade. Pick a boring, well-supported stack. This is not the place to prove a point with an exotic framework.

## Waiting for SOC 2 to sell

You do not need SOC 2 Type II to close your first ten customers, but you do need a credible plan and a Type I timeline. Have both ready in your first sales conversation.

# 6. About UZ Technologies

We are a senior product engineering team that has spent the last several years shipping healthcare software for US clinics, digital health startups and hospital innovation groups. Telemedicine platforms, patient portals, EHR and FHIR integrations, ambient AI clinical documentation, revenue cycle workflow, and the boring but critical audit, logging and access control plumbing that keeps all of it running.

We work in small, senior pods. No offshore hand-offs, no junior teams behind a senior sales pitch. The engineer who writes your code is on your standup, and they are the same person who explains it to your auditor.

### How we usually engage

Discovery sprint (1 to 2 weeks): we sit with your clinical and product team, map the workflow, list the compliance scope and hand back a fixed-fee proposal with a realistic timeline.

Build phase: senior pod, two week sprints, weekly demo, all code in your repository from day one.

Go-live and beyond: security hardening, third-party penetration test coordination, pilot support and a managed run-rate for the first year.

## Ready to talk

If you want a senior engineer to review your brief and send back a fixed-fee proposal with a compliance sketch and a realistic timeline, get in touch. First response within one US business day.

| | |
|---|---|
| Email | hello@uztechnologies.co.in |
| WhatsApp | +91 73000 30185 |
| Website | uztechnologies.co.in |
| Healthcare capabilities | uztechnologies.co.in/industries/healthcare |
| Book a call | uztechnologies.co.in/contact |

*This kit is provided for informational purposes and is not legal advice. For regulatory decisions specific to your product, consult qualified US healthcare counsel.*