CHECKLIST

A HIPAA-READY ARCHITECTURE CHECKLIST FOR CALL TEAMS

Tenant and location scope, server-side credentials, content-minimal logging, and an audit ledger, as questions to put to any vendor, including us.

AUGUST 14, 2026 · 8 MIN READ

A call team in a medical group touches protected health information every hour. The tools that team uses will each tell you they are HIPAA compliant. The phrase is not an architecture. It does not tell you what the vendor stores, what reaches a browser, or what you could produce if an auditor asked who called whom, when, and under what consent.

This checklist turns those questions into a list you can put to any vendor, including DialSplice. Each group ends with how we answer, so you can hold us to the same standard.

How to use this checklist

- Work through it with your compliance lead and your operations owner together. One knows the rules; the other knows how the work gets done.
- Ask for the mechanism, not the certificate. A vendor that can describe how scope is enforced on a request is telling you more than one that shows a badge.
- “No” and “we will check” are both answers. “It depends” is a question you have not finished asking.

- Compliance is shared. The last group is about your side of it.

Group 1: Tenant and location scope

A multi-location group has one contract and many clinics. A patient at one clinic must not be visible to an agent at another unless a role permits it.

- ☐ Does every request carry an organization and a location scope?
- ☐ What happens when the scope is missing, unknown, or ambiguous? Does the request fail, or does it fall back to a default?
- ☐ Can a location inherit another location’s credentials, caller ID, or data by accident?
- ☐ Is search filtered by role and location before results leave the server, or in the browser afterward?
- ☐ When a contact is seen at two locations, who sees both histories, and how is an ambiguous match handled?

How DialSplice answers: every request carries organization and location scope; unknown or ambiguous scope fails closed. An unknown location never inherits another’s credentials, caller ID, or data. Search results are filtered by role and location scope before they leave the server. A contact seen at two locations shows both histories only to roles scoped to both; an ambiguous match is held for a person, never guessed.

Group 2: Credentials

Provider tokens are the keys to your phone system, your CRM, and your EHR. Where they live decides what a compromised agent laptop can reach.

- ☐ Do provider credentials for telephony, CRM, or EHR ever reach the agent’s browser?

- ☐ How does click-to-call work? Does the vendor originate the call, or does the agent's own authenticated phone app?
- ☐ Does the vendor hold call audio at any point?
- ☐ Are credentials scoped per location, or shared across the organization?

How DialSplice answers: provider tokens live server-side and never reach the browser. Click-to-call hands a number to the agent's own authenticated phone app; DialSplice never originates the call and never holds the audio. The agent's browser only ever receives a work item.

Group 3: Content in logs and notifications

Alerts travel through third-party services: push, SMS, email, Teams, Slack. Logs travel to monitoring tools. Anything in either is outside your scope controls.

- ☐ What does a notification contain? Can it include a patient name, a phone number, or a message body?
- ☐ What do application logs contain? Are message bodies, transcripts, or recordings ever written to them?
- ☐ Is telemetry allowlisted by attribute, or does it capture whatever is in the request?
- ☐ Do exports, such as a call log CSV, carry message content?

How DialSplice answers: notifications carry no identity. A push says "Callback due · Northgate · 4:00 PM," never a name, a number, or a message body; opening it requires the workspace and the scope. Logs store events and hashes, not message bodies or recordings. Only allowlisted attributes leave the request path; identity and content never enter telemetry. The call log exports to CSV without message content.

Group 4: The audit ledger

The audit you cannot produce is the one spread across three vendors' logs, none of which you control.

- [ ] Is there a single append-only record of every action: claim, read, disposition, booking, configuration change?
- [ ] How would you detect that an entry was changed, removed, or reordered?
- [ ] Are denied actions recorded as well as permitted ones?
- [ ] What does a ledger entry contain, and what does it deliberately leave out?
- [ ] Can our compliance lead read it without asking the vendor to run a report?

How DialSplice answers: every event is written to a hash-chained, append-only audit ledger. Each event links to the previous by SHA-256, so changed, missing, or reordered history is detectable. Denied actions are recorded; a cross-clinic read that fails scope appears in the ledger as denied. The ledger stores events and hashes, not message bodies or recordings. Your compliance lead sees the ledger during rollout.

Group 5: External effects and reconciliation

A booking, an SMS, or a payment is an external effect. A retry that fires twice books twice or messages twice.

- [ ] Is every external effect journaled once, with an idempotency guarantee?
- [ ] What happens when a provider returns an ambiguous outcome, such as a timeout after the request was sent?
- [ ] Is an ambiguous outcome retried automatically, or held for a person?
- [ ] Are batch exports to a data platform journaled the same way?

How DialSplice answers: every effect is journaled once. An ambiguous provider outcome enters reconciliation, never a retry. A reconciliation hold is visible on the manager desk and released by a person. Every export batch is a ledger event with a hash; a failed batch is held for reconciliation, not silently retried.

Group 6: Access policy at runtime

A role assigned at login is only as current as the login.

- [ ] Is access validated at execution time, or only when the session starts?
- [ ] Which factors are checked: capability, scope, audience, environment, auth strength, expiry, revocation, session version?
- [ ] What locks an unattended workspace, and after how long?
- [ ] Can a revoked role still complete an action already on screen?

How DialSplice answers: capability, scope, audience, environment, auth strength, expiry, revocation, and session version are checked at execution time. Roles and scopes are validated at request time, not at login. Five-minute inactivity protection locks the workspace; unacknowledged alerts stay in an in-app recovery inbox.

Group 7: What is stored, passed through, and never returned

This is the question the BAA is about. Ask for three lists.

- [ ] What does the vendor store on its own systems?
- [ ] What does it read from our systems and pass through without storing?
- [ ] What does it never return to a browser, a log, or an export?
- [ ] Are recordings, transcripts, or clinical notes in any of the three lists?

How DialSplice answers, as three lists:

WE STORE	WE PASS THROUGH	WE NEVER RETURN
Work items, scope, timestamps, dispositions, event hashes, operational telemetry	Contact identity and history read from your CRM and system of record under your scopes	Recordings, transcripts, message bodies from the telephony adapter; provider tokens to the browser

Clinical notes and treatment history are never read. Notes written to the patient record are outcomes, not transcripts.

Group 8: Identity and booking

Two systems that disagree about the same person are a records problem and a safety problem.

- ☐ Before booking, does the agent see whether a patient record already exists, and at which locations?
- ☐ Is identity resolved before the booking writes, or reconciled afterward?
- ☐ When the EHR and the CRM both need updating, is it one event or two?
- ☐ What happens when the match is ambiguous?

How DialSplice answers: before booking, the agent sees whether the contact already has a patient record in your EHR, and at which locations, so nobody creates a duplicate. Bookings write to your system of record with identity resolved first; the CRM is updated from the same event, so the two never disagree. An ambiguous match is held for a person.

Group 9: Configuration change

Consent rules, quiet hours, attempt caps, and disposition lists are policy. A policy change without a record is a compliance gap.

- [ ] Is configuration versioned, with a content hash per revision?
- [ ] Are approval, activation, and rollback separate steps, each logged?
- [ ] Are readiness checks run before activation?
- [ ] Are scripts and guidance versioned and approved before agents see them?

How DialSplice answers: each configuration revision carries a content hash; approval, activation, and rollback are separate, logged steps. Readiness checks confirm locations mapped, roles and scopes assigned, consent and quiet-hours rules valid, and the disposition list present. Scripts and playbooks are versioned and approved before an agent sees them beside a contact. Notification policy is part of the same configuration.

Group 10: Contracts and posture

- [ ] Will the vendor sign a Business Associate Agreement?
- [ ] Where is the vendor on SOC 2? Ask for the current status, not the roadmap alone.
- [ ] Will the vendor walk your compliance lead through the architecture before you sign?
- [ ] Does the vendor document which responsibilities are theirs and which are yours?

How DialSplice answers: DialSplice is built HIPAA-ready and we sign a Business Associate Agreement with every medical customer. SOC 2 is in progress; ask us where we are today and we will share current status and roadmap. We will walk your security or compliance lead through the architecture, the ledger, and the data classes above before you sign. Compliance is shared; we document our controls and your responsibilities.

Group 11: Your side

No vendor architecture covers these. They are yours.

- ☐ Consent for each channel is defined and recorded somewhere the connector can read.
- ☐ Quiet hours, holidays, and attempt caps are written down per location.
- ☐ Roles list the locations they cover, and someone owns keeping that list current.
- ☐ One operations owner reviews and approves configuration revisions.
- ☐ Your telephony provider’s own recording and retention settings have been reviewed, since recordings stay there.
- ☐ Agents are trained that the workspace is the only place identity should appear, not a chat, a note, or an alert.

Reading the answers

A vendor that answers most of these with a mechanism is one you can audit. A vendor that answers with a certificate is asking you to trust the auditor instead. Bring the filled-in checklist to your compliance review, and bring your compliance lead to the demo.