



ProfitPad

HUBSPOT FOR HEALTHCARE

The HubSpot HIPAA Readiness Checklist

A self-audit for teams storing patient data in HubSpot.

Most healthcare teams on HubSpot assume that Enterprise plus a signed BAA means they are compliant. It doesn't. Compliance lives in the configuration, and the gaps stay invisible until an audit finds them. Run your portal through the list below. Every box you can't check is a gap, and gaps that involve PHI are the expensive kind to fix later.

This is an operational self-audit, not legal advice. Confirm your obligations with your own counsel.

Foundation

☐ **You have at least one Enterprise hub.**

Sensitive Data requires it. On Professional or below there is no configuration path to compliance.

☐ **Your BAA with HubSpot is signed.**

☐ **Sensitive Data is actually enabled, under Settings, then Privacy and Consent.**

Signing the BAA does not switch it on. Check the setting. Do not assume you are covered because you are on Enterprise.

PHI classification

☐ **Every PHI property is marked as sensitive.**

Date of birth, SSN, conditions, medications, treatment history, appointment details, and anything similar.

☐ **Each sensitive property was created sensitive from the start.**

The setting cannot be changed after a property exists, so a PHI value in a normal property has to be rebuilt, not toggled.

☐ **Identifiers are handled correctly.**

A name, email, or phone alone is not PHI. Tied to a diagnosis, medication, or treatment date, it is. The health fields get locked down.

☐ **Classification was done field by field, not by object or category.**

The obligation is triggered by the combination, so it is judged one property at a time.

Where PHI can and can't live

☐ **No PHI feeds the Custom Report Builder or Customer Journey Reports.**

Neither is covered for it.

☐ **No PHI is used in marketing emails or personalization tokens.**

☐ **No property that needs to reach Breeze AI carries PHI.**

Breeze cannot read sensitive properties, so anything marked sensitive is invisible to it, and anything left open to Breeze must not be PHI.

☐ **The clinical record lives in your EHR, not HubSpot.**

Full diagnosis and treatment history stay in the EHR. HubSpot holds the engagement layer only: demographics, communication, scheduling, referral tracking.

The shared-object test

☐ **Patients and B2B contacts are not on the same contact object with shared PHI properties.**

The most common and most damaging failure. Once they share an object, every property, report, and integration inherits the strictest constraint that applies to any record on it.

☐ **Consent tracking, if you do it, is built as a custom object rather than a pile of properties.**

Activities and access

- ☐ **PHI inside activities is access-controlled to the record owner.**
Calls, notes, one-to-one emails, meetings. Body content and attachments are covered, but coverage is not restriction. Access still has to be scoped.
- ☐ **Reps can see PHI only for the patients they own, not across the whole database.**

Integrations

- ☐ **No Zapier or Make touches any workflow carrying PHI.**
Neither holds a BAA that covers it.
- ☐ **Automation that moves PHI runs on a covered path.**
Native HubSpot workflows, or self-hosted automation such as n8n where the data stays in infrastructure you control.
- ☐ **The native Gmail or Outlook extensions are used with PHI only if your own mail is itself under a BAA.**

AI features

- ☐ **HubSpot NoteTaker is not running on meetings that capture PHI.**
It is not currently covered, though a HIPAA beta is planned.
- ☐ **AI features that are not zero-data-retention, including the support bot, are not processing PHI.**
- ☐ **Your team knows Breeze can summarize covered call and meeting content but cannot read sensitive properties.**

Reading your score

Everything checked.

Your architecture is sound. Keep the field-by-field discipline every time you add a property, because that is where drift starts.

One or two gaps.

Fixable, but close them before you layer more data or workflows on top. The longer a gap sits, the more gets built over it.

The shared-object box unchecked, or several boxes unchecked.

This is a remediation project, not a settings change. Do it in order: property audit first, then integrations, then re-architecture. Never re-architect first, because you cannot design the target state until you know which properties carry PHI and which integrations are writing it.

Found gaps you can't close on your own?

That is exactly the work we do.

[See how we build HubSpot for healthcare teams](#)