ALLGOOD

FREE PLAYBOOK

The Compliance Playbook for Behavioral Health Marketing

HIPAA, 42 CFR Part 2 & your EHR — what every treatment center should understand before running another ad.

A plain-English field guide for operators and marketing teams. No legalese, no fluff — just the rules that touch your marketing, the mistakes that create risk, and the questions that separate a real partner from a liability.

2026 Edition · Allgood Marketing · Fort Lauderdale, FL · Serving behavioral health nationwide

INTRODUCTION

Marketing is now a compliance problem

For most of marketing history, compliance was the clinical team's job and marketing lived safely on the other side of the building. In behavioral health, that wall is gone.

The moment your marketing systems touch patient data — a form fill, a tracking pixel, a call recording, a CRM synced to your EHR — compliance becomes a marketing problem too. And the regulators have noticed. Over the past few years, a wave of enforcement has hit healthcare organizations not for what their clinicians did, but for what their **websites and ad pixels** were quietly sending to Google and Meta.

For addiction treatment and behavioral health specifically, the stakes are higher than almost anywhere else in healthcare. You operate under a federal confidentiality rule stricter than HIPAA, you serve a vulnerable population, and you compete in a market full of agencies selling cheap leads with no idea that any of this exists.

This playbook is the short, honest version of what you need to know. Read it once and you'll understand more about marketing compliance than most agencies pitching you ever will.

> **WHAT YOU'LL TAKE AWAY**
>
> The handful of rules that actually touch your marketing, the single biggest risk hiding on your website right now, the agreements you need before data flows, and a checklist plus ten questions you can use the next time an agency tries to win your business.

SECTION 1

HIPAA for marketers — the 90-second version

You don't need to be a privacy lawyer. You need to know what counts as protected data and when your marketing touches it.

What counts as protected health information (PHI)

PHI is any information that links a person to their health, care, or payment for care. In a treatment-center context, that includes the obvious (names, diagnoses, admission records) and the less obvious: an IP address tied to a visit to your "verify your insurance" page, a phone number captured on an intake call, or a form submission asking about detox.

When your marketing touches it

More often than teams realize. The common pressure points:

- **Website forms and chat** that capture contact details and care interest.
- **Tracking pixels and analytics** that broadcast on-page behavior to ad platforms (see Section 3 — this is the big one).
- **Call tracking and recordings** that capture identifiable patient conversations.
- **CRMs and dashboards** that pull or store admission and contact data.

The "business associate" idea

If a vendor (including a marketing agency) creates, receives, maintains, or transmits PHI on your behalf, they're a **business associate** — and they must sign a Business Associate Agreement (BAA) before any of that data flows. An agency that doesn't know what a BAA is should never be near your patient data.

> **THE OPERATOR TAKEAWAY**
>
> You don't have to memorize the regulation. You have to make sure every vendor who can see patient data has signed the right agreement and knows how to handle it. If they can't speak to this fluently, that silence is your answer.

SECTION 2

42 CFR Part 2 — the stricter rule for SUD

If you treat substance use disorder, a second federal rule sits on top of HIPAA — and it's tougher. Ask your marketing agency what it is. A blank stare is worth paying attention to.

What it is

42 CFR Part 2 is the federal rule protecting the confidentiality of substance use disorder treatment records held by federally assisted programs. It exists because the consequences of a SUD record leaking — stigma, lost employment, legal exposure — are uniquely severe. In important ways it is **stricter than HIPAA**, particularly around consent and re-disclosure.

What changed in the 2024 Final Rule

Part 2 was substantially revised in a 2024 Final Rule that brought it into closer alignment with HIPAA. The headline changes operators should know:

- **Single consent.** A patient can now provide one consent for all future uses and disclosures for treatment, payment, and health care operations (TPO), rather than re-consenting at every step.
- **HIPAA alignment.** Breach-notification expectations and several definitions were harmonized with HIPAA, simplifying compliance for organizations already doing HIPAA.
- **Enforcement teeth.** Enforcement authority sits with the same federal office that enforces HIPAA (the HHS Office for Civil Rights), and active enforcement of the updated rule is now in effect.

Why it matters to marketing

Because the same data that's most valuable for proving marketing actually works — who inquired, who admitted, through which channel — is exactly the data Part 2 protects most tightly. The answer is not to avoid the data. It's to get safely close to it, inside a compliant boundary, with the right consents and agreements in place. Agencies that understand this can optimize to real outcomes. Agencies that don't either avoid the data entirely (and keep guessing) or touch it carelessly (and create liability).

> **RISK FLAG**
>
> Standard advertising tools were not built with Part 2 in mind. Bolting a generic marketing stack onto a SUD facility's website is how well-meaning teams create exposure without realizing it.

Regulatory summaries here reflect the 2024 Final Rule as understood at publication and are simplified for operators. They are not legal advice — confirm current requirements and your specific obligations with qualified counsel.

SECTION 3

The website tracking trap

This is the single most common — and most overlooked — compliance risk in behavioral health marketing. It's probably live on a site right now.

How a pixel leaks data

Standard advertising and analytics pixels (the snippets that power Google and Meta ad targeting and conversion tracking) work by sending visitor data from the browser straight to the ad platform. On an ordinary e-commerce site, that's routine. On a **patient-facing treatment site**, it can mean shipping protected information — what pages someone viewed, what they searched, that they submitted an insurance-verification form — to third-party advertising companies. That data transfer is exactly what triggered a wave of enforcement actions and litigation against hospitals and health systems.

What compliant tracking looks like

The goal isn't to fly blind. It's to measure marketing without broadcasting PHI. In practice that means:

- **Server-side tracking** — data is routed through a server you control instead of firing directly from the visitor's browser to ad platforms, so you decide what is shared.
- **De-identification** — identifiers are stripped or hashed before anything leaves your boundary, so conversions can be measured without exposing the person.
- **A defined data boundary** — clear zones for what is identifiable, what is de-identified, and what is allowed to reach a third party.

> **DONE RIGHT, YOU STILL GET THE DATA**
>
> Compliant tracking is not "less measurement." Built correctly, it gives you cleaner attribution than a leaky pixel ever did — because it's tied to real outcomes inside your systems rather than guessed at by an ad platform.

> **CHECK THIS TODAY**
>
> Ask whoever runs your website: are standard Meta and Google pixels firing on pages where patients enter information? If the answer is yes — or "I'm not sure" — that's the first thing to fix.

SECTION 4

The two agreements you need: BAA & QSOA

Before any patient data flows to a marketing partner or tool, two agreements should be in place. For SUD programs, you need both — not one.

Agreement	Which rule	What it does
BAA Business Associate Agreement	HIPAA	Binds a vendor that handles PHI on your behalf to safeguard it, use it only as permitted, and report breaches. Required for any business associate.
QSOA Qualified Service Organization Agreement	42 CFR Part 2	Required when a service organization needs access to Part 2-protected SUD records to provide its service. The Part 2 counterpart to a BAA.

A HIPAA-covered marketing partner working with a SUD program generally needs to be both a business associate **and** a qualified service organization — which means **both** a BAA and a QSOA, executed before the first record is shared. Operational readiness (encryption, access controls, a written breach-response plan) should be in place at the same time.

> **A SIMPLE GATE**
>
> No agreements, no data. Treat signed BAA + QSOA as a hard prerequisite — the gate that opens only after a partner has proven they can be trusted with the most sensitive records you hold.

SECTION 5

EHR integration, done right

Compliance isn't only about avoiding risk. Done well, it unlocks the one thing that actually tells you whether your marketing works: your admission data.

Why connect to your EHR at all

The metric that reflects your business isn't cost-per-lead — it's **cost-per-verified-admit**: what you spent to produce one paying admission. That number lives in your EHR (Kipu, Sunwave, Alleva), not in your ad account. Connecting marketing data to admission data — safely — is what turns "we got you cheap leads" into "here's what each channel actually cost you per admit."

What "done right" means

- **Read-only access** scoped to exactly what's needed — no more.
- **A compliant boundary** where identifiable matching happens inside your protected zone, and only de-identified results (e.g., cost-per-admit by channel) ever leave it.
- **Matching on minimal keys** (such as a phone number) to connect a marketing source to a verified admit, then discarding what isn't needed.
- **The right agreements first** (Section 4) and a written breach plan before any data flows.

What it unlocks

- **True cost-per-admit by channel** — so you cut spend that produces inquiries but not admissions, and double down on what fills beds.
- **Census-aware pacing** — adjust spend to your actual bed availability instead of burning budget while you're already full.

> **THE COMPETITIVE TRUTH**
>
> Most agencies can't do this — not because the idea is hard, but because EHR access requires compliance fluency and the facility's trust, and the agencies competing on cheap leads can't credibly ask for either. The compliance work isn't the obstacle. It's the key to the door.

SECTION 6

Florida note: how your agency is paid

If you operate in Florida, one more rule shapes how a marketing relationship should be structured — and it's about money, not data.

Florida's Patient Brokering Act restricts paying or receiving compensation in exchange for patient referrals. In a marketing context, that's why a fee structure tied to **per-lead** or **per-admission** payments can create real exposure for SUD providers. A partner who knows the space prices differently:

- **Flat-fee retainers, set in advance** — you pay for a defined scope of work, not for patient volume.
- **Ad spend as a separate, client-paid pass-through** — not a referral-contingent fee.
- **Cost-per-admit as a reporting metric you optimize against — never the basis on which you're billed.**

> **WHY THIS IS ACTUALLY GOOD NEWS**
>
> The safe structure and the smart structure point the same way: a flat-fee partner accountable to your outcomes, not a broker selling you bodies. If an agency proposes paying them per lead or per admit in Florida, treat it as a red flag, not a bargain.

This is a simplified summary of one state's law and is not legal advice. Fee structures should be reviewed by qualified Florida healthcare counsel before you sign.

SECTION 7

Your compliance checklist

A practical starting point. Work through it with your marketing lead and your compliance officer — and bring counsel in where noted.

- ☐ **Audit your pixels.** Identify every tracking script on patient-facing pages; confirm none are sending identifiable data to ad platforms.
- ☐ **Move to server-side, de-identified tracking** for conversions on patient-facing pages.
- ☐ **Inventory where patient data lives** across forms, chat, call tracking, CRM, and dashboards.
- ☐ **Confirm a signed BAA** with every vendor that can touch PHI.
- ☐ **Confirm a signed QSOA** with every vendor that can touch Part 2 SUD records.
- ☐ **Verify consent language** supports your intended uses under the 2024 Part 2 rule (with counsel).
- ☐ **Put a written breach-response plan in place** before you need it.
- ☐ **Scope EHR access to read-only** and define your data boundary and zones.
- ☐ **Review your agency's fee structure** against state patient-brokering law (with counsel).
- ☐ **Re-run this checklist** whenever you add a tool, a vendor, or a new landing page.

SECTION 8

10 questions to ask any marketing agency

The wrong partner doesn't just waste budget — they can expose you to risk. These questions separate real partners from vendors. The right ones answer all ten without flinching.

1. **"What's our cost-per-admit — not cost-per-lead?"** Leads are noise; admits are revenue. If they only talk leads and clicks, they're guessing about the thing that matters.

2. **"How do you know a lead actually became an admit?"** The honest answer involves connecting marketing data to your admissions reality inside a compliant boundary. Most can't answer at all.

3. **"What is 42 CFR Part 2, and how does it affect our marketing?"** If they've never heard of it, that's your answer.

4. **"Are standard pixels firing on our patient-facing pages?"** Ask specifically about website tracking and patient data — the wrong setup is a documented liability.

5. **"Will you sign a BAA and a QSOA?"** A blank look here means they don't belong near your data.

6. **"How is your fee structured?"** In Florida especially, paying per lead or per admission can run into patient-brokering law. A partner who knows the space bills flat-fee and can explain why.

7. **"How do you keep us able to advertise — LegitScript, platform policies?"** Getting and keeping certification and ad-account approval in this vertical is its own skill.

8. **"Do you pace spend to our census?"** Spending hard while you're full is wasted budget. A sophisticated partner adjusts to bed availability.

9. **"Where does our patient data physically go, and who can see it?"** They should be able to draw you the map.

10. **"When AI makes campaign-building basically free, what's your edge?"** The agencies that survive won't compete on execution alone — they'll compete on data, outcomes, and access AI can't replicate.

> **USE IT**
>
> Print this page. Bring it to your next agency call. The right partner will be glad you asked; the wrong one will change the subject.

FINALLY

Compliance is a feature, not a landmine

The point of this playbook isn't that marketing in behavioral health is dangerous. It's that it rewards expertise.

The agencies that understand HIPAA, 42 CFR Part 2, and how to wire safely into your EHR can do something the cheap-lead shops can't: get close to your real outcomes, advertise without creating liability, and tell you what your marketing actually costs you per admit. Compliance fluency isn't a nice-to-have. It's the thing standing between effective marketing and a regulatory headache.

This playbook is educational and reflects a general, simplified understanding of the referenced regulations as of its 2026 publication. It is not legal advice, does not create an attorney–client or advisory relationship, and should not be relied on for compliance decisions. Confirm your specific obligations with qualified healthcare counsel before acting.