Freshpaint

THE NEW RULES OF DTC:

Pharma & Med Device Marketers' Guide To Growth Without Risk *

Table of Contents

The Boom and the Blind Spot

Direct-to-consumer (DTC) marketing for pharma and med devices is surging. From branded websites and co-pay programs to telehealth and fulfillment flows, the push to reach patients directly is accelerating faster than ever.

But there's a big, problematic elephant in the room: privacy risks. The same funnels that drive growth are also where sensitive data, including PHI, can leak most easily. And it doesn't even matter if HIPAA applies to your organization or not. Regulators are watching, regardless of your HIPAA status. Plaintiffs' attorneys are, too. And marketers are starting to wake up to the real risks here.

A recent AdExchanger/PurpleLab survey highlights just how unsteady the ground has become:

Description	Percentage
Healthcare and pharmaceutical advertisers who admit they're only moderately to not at all prepared for state-level privacy changes	57%
Respondents who have already dropped vendors in the past year due to privacy concerns	20%
Healthcare advertisers who have reallocated spend away from audience targeting and toward contextual placements in response to tightening privacy rules	43%

Translation: Pharma and medical device marketers feel vulnerable. Compliance teams are nervous. And vendor instability is already costing money, time, and momentum.

The other pressure point is performance itself. Advertisers know they can't afford blind spots, but **confidence in measurement is eroding fast:**

Description	Percentage
Advertisers who say they're only moderately confident in their DTC measurement	53%
Respondents who feel very confident in their ability to measure effectively	13%

Fragmented channels such as social, CTV, programmatic, and endemic sites make it nearly impossible to connect the dots from clicks to real business outcomes. Marketers are left guessing whether their spend is driving scripts, device adoption, or just resulting in wasted impressions.

The old reliance on third-party pixels and trackers is no longer sustainable. But that doesn't mean growth has to slow. That's where this guide comes in. We'll help you identify the biggest privacy risks hiding in your DTC funnel and map out a privacy-first approach that protects patient data and proves the impact of every ad dollar.

Why HIPAA Exemptions Don't Mean Safety

Pharma and med device marketers often lean on a common assumption: *If we're not a HIPAA-covered entity, we're safe.* That assumption no longer holds. Regulators, legislators, and plaintiffs' attorneys are making it clear that HIPAA exemptions don't protect DTC funnels from scrutiny.

Even without HIPAA obligations, your marketing data can still trigger state privacy laws. HIPAA protects a narrow set of identifiers, while state laws reach much further—covering personal and behavioral data tied to health context. The chart below shows why "HIPAA-exempt" doesn't mean "risk-free."

HIPAA PHI

Individually identifiable health information created or maintained by a HIPAA covered entity or business associate

- Name
- Email address
- Address (including geographic subdivisions smaller than state)
- Dates (except year) directly related to an individual including date of birth, date, admission, procedure, or age > 89
- Numbers (telephone, fax, financial account, medical record, health plan beneficiary, SSN, driver's license, passport, account, certificate, license plate, serial, etc.)
- Device identifiers including GAID/IDFA
- IP Addresses and URLs
- Full-face photographic and comparable images
- Biometric identifiers such as fingerprints
- Any other unique identifying number, characteristic, or code including cookie/pixel IDs, customer IDs

State Consumer Privacy "Personal Data"

In addition to all HIPAA PHI, state definitions of personal data or personal information may include:

- Precise geolocation (outside the HIPAA context)
- Browsing behavior & purchase history
- Demographics (e.g., age, gender) (Note: "age > 89" is a PHI identifier when linked to health info)
- Inferences/profiles (interests, propensities)
- Employer, job title, education (non-FERPA)

The FTC Is Watching

GoodRx learned this the hard way: a $1.5M FTC fine and permanent ban on sharing health data with ad platforms. That ban didn't just mean legal exposure. It cut off GoodRx's ability to retarget, personalize, and measure across the biggest growth channels. The company lost the marketing signals it relied on to drive acquisition, undermining both performance and investor confidence. And if that wasn't enough, following the FTC fine, GoodRx was hit with a $25M class action settlement for the same violations.

The FTC's case set a precedent: you don't need to be a HIPAA-covered entity to face steep penalties if your marketing practices mishandle sensitive health information.

Pixels in the Crosshairs

And GoodRx isn't the only non-HIPAA covered entity facing a class action lawsuit over pixel usage. A leading pharmaceutical company is facing lawsuits over the use of tracking pixels in co-pay support programs, where plaintiffs argue that data sharing with ad platforms exposed sensitive patient details.

What used to be a "standard" funnel tactic is now a legal liability waiting to happen.

Lawmaker Attention on DTC Pharma

DTC pharma marketing has been explicitly flagged in the Senate DTC Probe, with lawmakers zeroing in on how data flows through telehealth redirects and financial support programs. Now the executive branch has joined the scrutiny. On September 9, 2025, President Trump signed a memorandum directing the FDA and HHS to crack down on misleading direct-to-consumer prescription drug ads—especially on social media, online pharmacies, and other digital channels.

This puts the entire DTC model (awareness campaigns, co-pay cards, telehealth redirects, fulfillment) under the microscope. Not just for performance, but for transparency, risk disclosure, and legal compliance.

States Raising the Bar

The recent Healthline Media settlement in California shows just how far regulators are willing to stretch the definition of "sensitive health data." It's no longer limited to diagnoses. Even browsing behavior and article titles (e.g., "If you have HIV, this is what you should know") can be treated as protected health information.

For pharma and med device marketers, this creates two major risks:

- **Content framing:** Educational headlines and awareness pages that directly imply a condition can trigger state-level enforcement.
- **Vendor exposure:** Contracts with publishers, platforms, and partners must now spell out opt-outs, data-sharing limits, and purpose limitation clauses.

California regulators invoked the purpose limitation principle under CCPA to penalize data use that inferred health status. This "blueprint" could spread to other states. For pharma marketers, that means your entire DTC ecosystem can be viewed as one continuous data chain under your compliance obligations.

The takeaway: Purpose limitation isn't obscure legal language anymore—it's a design constraint for DTC marketing.

"California's action in Healthline changed the risk profile for any business advertising in the health space. It introduced more regulators, making increased enforcement likely, and applied a new tool: the purpose limitation requirement. Compliance is no longer just about doing what you say. It's now judged against whether a data use aligns with consumer expectations, giving regulators more power and raising risk for healthcare advertising."

Mason Fitch
Hintze Law PLLC

Bottom Line

Whether you're in pharma or medical devices, HIPAA exemptions won't protect you from today's privacy landscape. FTC rules and state laws both apply—and they're already being enforced.

Consent Isn't Always Compliance

A cookie banner or consent management platform (CMP) alone doesn't stop sensitive data from leaking. It just records preferences while pixels and trackers often fire anyway. Regulators don't care how pretty your banner is; they care whether you blocked, anonymized, and governed the data at the source.

Freshpaint protects privacy at the data layer, replacing non-compliant trackers with a safe, compliant Freshpaint pixel. Sensitive information is stripped automatically, and every data flow is audited in real time. For pharma and med-device marketers, compliance moves beyond banners to become part of the infrastructure—real protection for patients and brands alike.

"A cookie banner or consent management platform is a great step, but it is not a 'magic bullet.' Significant risk exists if an organization says on their website that they do one thing, but then they actually do the opposite. This has been a common assertion in federal and state enforcement action, as well as class action lawsuits (e.g., an organization promises not use it for advertising purposes without consent, but then does indeed use it for advertising purposes; or an organization uses a consent manager and an individual has turned off consent, and then the organization uses their data anyway)."

Jen Pike
Alston & Bird

Funnel Stage Risks: Where Pixels Leak PHI

For pharma and med device marketers, risk isn't theoretical. It's baked into the campaigns you run every day. Each stage of the marketing funnel, from awareness to fulfillment, creates opportunities for sensitive patient data to leak if third-party trackers are left in place.

The following breakdown maps out the risks, real-world examples, and practical audit steps compliance teams can start using today.

How We Assessed Risk Levels

Each stage of the funnel was evaluated against three factors:

- **Type of data exposed** — does the stage involve contextual signals (e.g., condition-implying page visits), or explicit PHI such as prescriptions, diagnoses, or insurance details?
- **Likelihood of tracker exposure** — how common is it for pixels or tags to be embedded in this type of flow, and how easily can they capture sensitive data?
- **Regulatory and legal precedent** — have regulators, courts, or plaintiffs' attorneys already flagged this type of funnel as a violation?

- A "**Medium**" rating indicates contextual exposure that can infer health status.
- "**High**" reflects direct PHI capture with significant litigation risk.
- "**Very High**" applies to stages where PHI is both unavoidable and under active regulatory scrutiny, making pixel exposure nearly indefensible.

Branded Sites (Awareness & Education)

Risk Level: Medium

Why it's risky: Landing on a branded drug or device page could be considered revealing of a diagnosis or health condition. Pixels on these pages can pass that sensitive context to Meta, Google, or other platforms.

"What we are learning from state consumer protection enforcement action in this space is that regulators are making a connection between the types of materials a user might view on a webpage to the realities of that user."

Jen Pike
Alston & Bird

"The lines around what counts as sensitive health data are still being drawn. The ambiguity itself creates risk on top of the ongoing risk related to advertising in healthcare."

Mason Fitch
Hintze Law PLLC

Examples:

- **Leading Ulcerative Colitis Drug:** A patient who clicks a Meta ad and lands on branded drug's ulcerative colitis page is automatically signaling a potential diagnosis. If a tracking pixel fires on that page, it ties a sensitive GI condition to an individual user profile.
- **Leading Ankle Replacement Device Company:** A leading orthopedic medical device company's *"Is it time to consider Total Ankle Replacement?"* page is designed to educate patients about surgery options. But a visit to this type of product page strongly infers an orthopedic condition. With pixels in place, that intent data can be shared with platforms that were never meant to handle PHI.

Audit Checklist:

- ☐ Audit all pixels/tags for PHI-adjacent exposure
- ☐ Confirm consent banners provide granular control
- ☐ Transition to anonymized tracking

Co-Pay Program (Financial Assistance)

Risk Level: High

Why it's risky: Enrollment flows capture prescription, insurance, and diagnosis details — data that courts treat as PHI. If trackers touch this information, lawsuits follow.

"Prescription and insurance information is very sensitive – prescriptions can reveal a lot about an individual and insurance information can be used for fraudulent purposes. So, protecting this type of information and using it in a compliant manner is very important."

Jen Pike
Alston & Bird

"The sensitivity of personal information is a function of how certain you are of a consumer's identity and how certain you are that their actions relate to their own health condition. When a site is collecting information such as prescription information and insurance details, there's more certainty that you have information specific to an identifiable individual's health condition."

Mason Fitch
Hintze Law PLLC

Examples:

- **Leading Drug that lowers LDL-C:** Patients who click through ads to access a cholesterol drug co-pay card must provide insurance and prescription details to enroll. That flow directly captures PHI, and if trackers are firing, those sensitive data points could be exposed to third parties.
- **Leading CGM Device Rebate/Warranty:** Device makers who ask patients to submit device serial numbers and health condition details when registering for warranty or rebate programs. Those forms are goldmines of PHI, and risky trackers embedded in the flow create a direct compliance exposure.

Audit Checklist:

- ☐ Review enrollment data flows for PHI exposure
- ☐ De-identify prescription and diagnosis data before processing
- ☐ Validate consent capture for sufficiency and clarity

Telehealth Redirects (Virtual Care Intake)

Risk Level: Very High

Why it's risky: Redirects from branded sites to telehealth partners or device trial kits create cross-domain tracking risk. If pixels fire here, it can trigger HIPAA BAA obligations.

"Any information sharing between two health entities is risky—especially when the handoff happens on a condition-specific page.. Even if HIPAA does not apply, the risk here is similar to the risk in other healthcare contexts—if you're sharing information that implies a certain health condition or diagnosis, you may need consent to do so. In the calculus of whether a certain user action implies that they have a health condition, a handoff to a healthcare provider site is likely more high risk than a handoff to, for example, an informational site."

Mason Fitch
Hintze Law PLLC

Examples:

- **Leading DTC Pharma Company with GLP-1 drug:** Clicking from a branded pharma DTC platform page for a GLP-1 prescription involves a cross-domain redirect into a telehealth partner flow. If pixels fire during this handoff, it exposes patient intent data at the precise moment they're seeking treatment—a scenario that often requires a HIPAA BAA.
- **CGM Free Trial Kit:** Patients can request a CGM trial kit directly online, with the company coordinating the prescription request on their behalf. This creates a direct PHI exchange. If marketing pixels are active in this flow, they capture clinical data alongside consumer intent.

Audit Checklist:

- ☐ Map the full patient journey across brand and partner domains
- ☐ Confirm HIPAA obligations with partners; secure BAAs if required
- ☐ Separate marketing tracking from clinical intake or adopt HIPAA-compliant infrastructure

Pharmacy Fulfillment (Rx)

Risk Level: Very High

Why it's risky: Prescription and device fulfillment inherently involve PHI. Tracking with adtech tools exposes the most sensitive stage of the funnel to regulators and plaintiffs.

"Regulators and plaintiffs are very protective of this type of information. The fact that the information is so sensitive gives rise to claims of greater harm, and thus, more significant enforcement measures, whether that is advertising bans or seven figure settlements imposed by regulators, or increased monetary demands from plaintiffs."

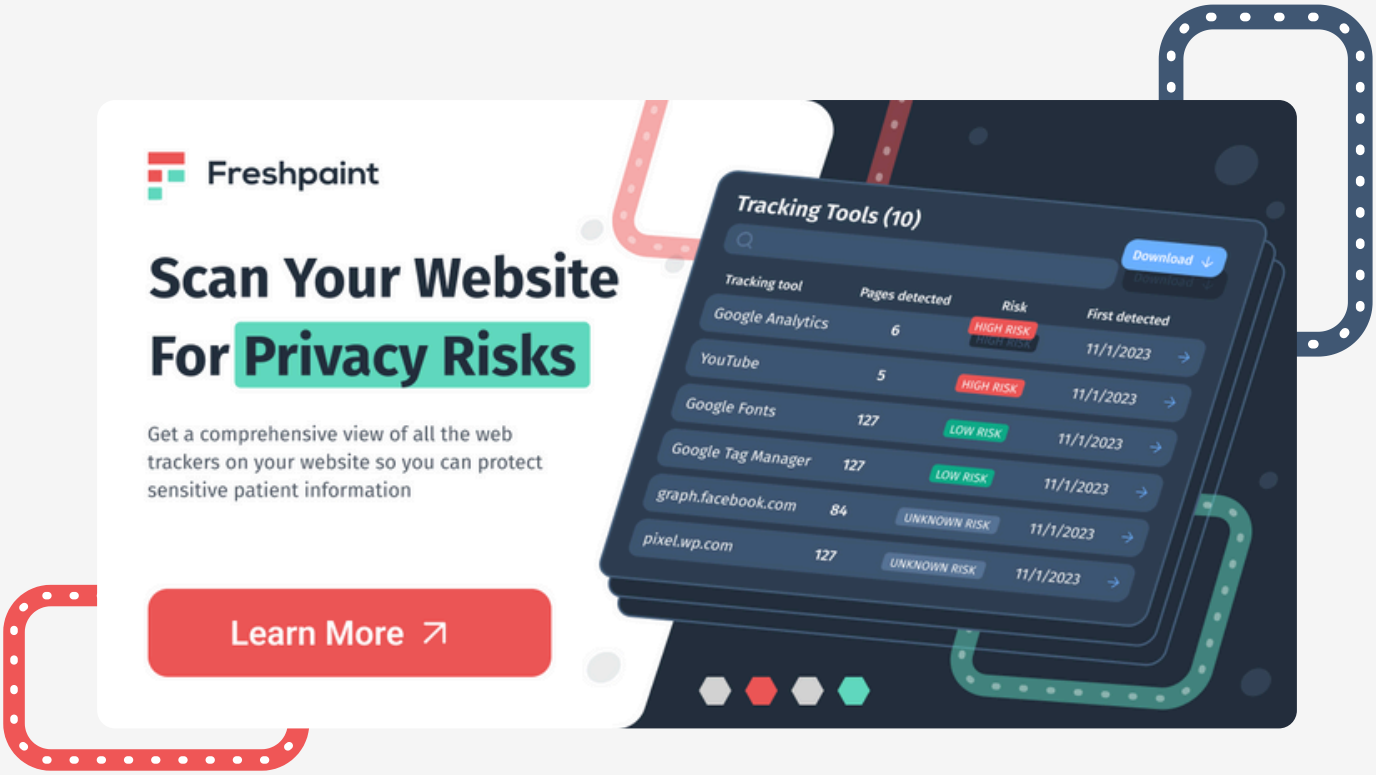
Jen Pike
Alston & Bird

Examples:

- **Leading GLP-1 Pharmaceutical Company:** A patient support program run by a leading pharmaceutical company offers resources like co-pay assistance, medication guidance, and patient education for people using its diabetes and obesity medications. Its online portal supports patients filling prescriptions for a popular GLP-1 drug. If trackers are present on this portal, fulfillment data tied to a specific condition and prescription could flow directly to ad platforms — exactly the type of exposure regulators have penalized.
- **Leading Hearing Aid and CGM Companies:** Some medical device manufacturers offer direct-to-consumer online ordering for their products. When tracking pixels or analytics tags are present on these portals, usage and fulfillment data about specific devices and health conditions can be transmitted to third parties. This creates the potential for violations of HIPAA and state privacy laws if the data is linked back to an identifiable patient.

Audit Checklist:

□ Audit fulfillment flows end-to-end for tracker exposure
□ Confirm no PHI leaves the ecosystem for ad platforms
□ Validate HIPAA and state-level compliance (e.g., WA MHMDA, CA CPRA)



The Takeaway

Every funnel stage, from awareness pages to fulfillment, could be a regulatory landmine if privacy isn't prioritized. The exposure isn't theoretical; it's happening today across both pharmaceutical and medical device marketing campaigns.

The path forward is clear: Replace risky pixels with privacy-safe infrastructure. That's how marketers preserve measurement, attribution, and growth without exposing patients or their brands.

The Freshpaint Advantage

Marketers shouldn't have to choose between protecting patient data and hitting their growth goals. Freshpaint was built for exactly this challenge.

Privacy-First by Design:

Freshpaint's Healthcare Privacy Platform replaces risky third-party pixels with a governance layer that gives you control over what data is shared, when, and how. Instead of platforms deciding what to collect, you decide what leaves your ecosystem.

Control the Data Flow:

Most pixels leak data the moment they load. Freshpaint works the opposite way: no data leaves your environment unless you explicitly allow it. That control lets you measure every step of the funnel without exposing PHI, while compliance teams stay confident that nothing slips through the cracks.

Performance Without Compromise:

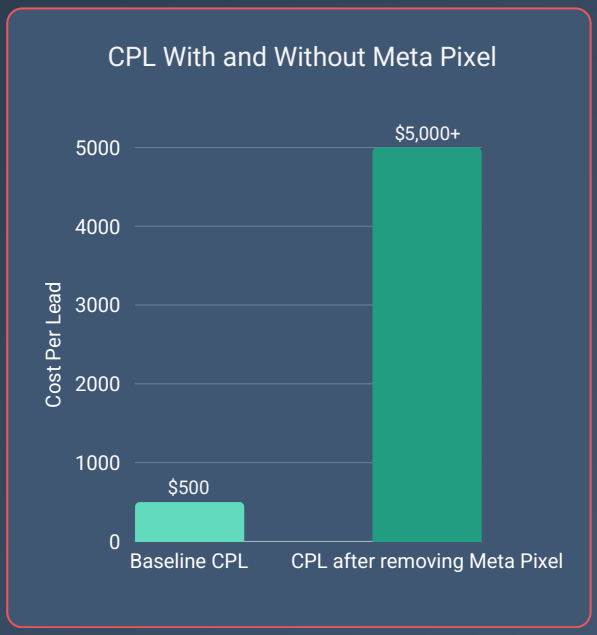
With Freshpaint, you don't sacrifice growth for compliance. You regain the attribution signals needed to optimize campaigns across Meta, Google, CTV, and beyond. The result: smarter spend, stronger performance, and patient trust intact.

Case Study: Global Diabetes Med Device Brand

Challenge

When the diabetes division of a major medical device company was forced to remove the Meta Pixel for compliance reasons, the fallout was immediate.

- Forced to remove Meta Pixel for compliance.
- Leads ↓ ~90%
- CPL: $500 → $5,000+
- Team refused to abandon DTC; needed a new, compliant growth engine.



Solution

They partnered with Freshpaint to implement HIPAA-compliant tracking, restored lost leads on Meta, and uncovered new lead-gen opportunities on TikTok.

Results

- Lead recovery on Meta
- CPL back to baseline
- New acquisition on TikTok with confidence to expand to LinkedIn, Google Ads, Bing, and Reddit.
- Team now scales with compliance baked in, not bolted on.

From Clicks to Care, Safely

Pharma and med device marketers face a clear choice: keep relying on third-party pixels and risk regulatory blowback, or adopt privacy-safe infrastructure that protects patients and marketing performance.

The truth is, you don't have to pick one or the other. With the right framework, you can measure every ad dollar—from clicks to scripts, from leads to device adoption—without leaking PHI, a true win-win. Freshpaint helps life science brands safeguard their funnels while restoring the attribution and optimization signals they need to grow.

Request a DTC Funnel Privacy Audit to uncover hidden risks, map out exposures across your funnel, and see how privacy-first tracking can fuel compliant growth.

Keep Learning

Freshpaint enables pharmaceutical and medical device companies to unlock performance marketing while staying compliant with a growing list of privacy laws. By replacing non-compliant tracking tools, Freshpaint empowers marketing teams to accurately measure campaign performance, target the right patients, and improve ROI, all with regulatory compliance baked in. Better insights. Smarter campaigns. Privacy-first by design.

Visit **Freshpaint.io**

Contact us at **sales@freshpaint.io**

Connect with us on **Linkedin**

Meet with us