A BEGINNER'S GUIDE

Meta Ads and HIPAA

How healthcare advertising leaks patient data, and how to advertise safely



Ibrahim Jaafar · Not legal advice

THE SHORT ANSWER

Meta won’t sign a BAA, so patient data must never reach Meta

You can still advertise on Facebook and Instagram.

But keeping PHI away from Meta is **your** job, not Meta’s.

ROADMAP

What we'll cover

1	**How data reaches Meta**	Pixel, Conversions API, Lead Ads, audiences
2	**The risks**	What leaks, and Meta's own rules
3	**Real cases and the rules**	What happened, and what applies today
4	**Advertising safely**	Practical steps and a checklist

1

PART 1 OF 4

How data reaches Meta

Meta’s advertising tools, in plain words

1 · HOW DATA REACHES META

Meta’s three advertising tools

IN THE BROWSER

Meta Pixel

A snippet of code on your website. It reports page visits, clicks and form fills to Meta, by default.

FROM YOUR SERVER

Conversions API

Your server tells Meta about actions, like a sign-up. You choose exactly what is sent.

ON META ITSELF

Lead Ads and audiences

Forms filled inside Facebook, and customer lists you upload to target or find “lookalikes”.

Key difference: the Pixel sends whatever it sees; the Conversions API sends only what you choose.

How one click becomes a leak

A patient clicks “Book”

`clinic.com/oncology/book-appointment`

→

The Pixel sends

- The full page address
- The visitor’s IP address
- Their Facebook cookie
- Buttons clicked, form fields

→

Meta

Matches it to the person’s Facebook account

Put together: “This named person is booking a cancer appointment.” That’s PHI.

2

PART 2 OF 4

The risks

What leaks, and Meta’s own rules

2 · THE RISKS

Four ways patient data reaches Meta

Pixel on sensitive pages

Patient portals, booking flows and symptom forms send URLs, clicks and typed details.

“Hashed” data that still matches

Scrambled emails or phones are matched back to real accounts by Meta. Hashing isn’t anonymous.

Patient-list audiences

Uploading patient lists for targeting or “lookalikes” tells Meta who your patients are.

Booking events tied to a person

A booking at a diabetes clinic reveals a patient, whatever the event is called.

Meta’s own rules on health data

Its terms forbid it

Meta’s Business Tools Terms say advertisers must not send health information.

It filters some data

Meta says it tries to block sensitive health data from its ad systems. Don’t rely on it.

Since 2025: limits for health advertisers

`Core setup`	Only the website domain is shared, not the full page address or custom details
`Partial`	Lower-funnel events like purchases or bookings are blocked
`Full`	All events from the website are blocked

Remember: these rules protect Meta. HIPAA responsibility stays with you.

If patient data does reach Meta

WHAT YOU MUST DO

1. **Stop the leak and investigate**
   Remove the tracking, find out what was sent, and about whom.
2. **Tell every affected patient**
   In writing, within 60 days of finding the breach.
3. **Report it to the regulator**
   500+ people: within 60 days. Fewer: in a yearly report.
4. **Tell the media if it’s big**
   Required when 500+ people in one state are affected.

WHAT IT CAN COST

HIPAA fines

$145 to $73,011 per violation, up to $2.19M a year per type. Careless = higher.

Criminal charges

Knowingly misusing PHI can mean jail, up to 10 years.

Lawsuits and FTC

Patient settlements of $6.6M–$12.2M; FTC fines of $50,000+ per violation.

Years of monitoring

Settlements usually add a corrective plan the regulator checks.

3

PART 3 OF 4

Real cases and the rules

What happened, and what applies today

What happened, 2022 to 2024

Aug 2022	**Novant Health** tells 1.3M patients a misconfigured Pixel may have sent data to Meta. Later settles for $6.6M.
Oct 2022	**Advocate Aurora Health** reports up to 3M patients affected by pixels on portals. $12.2M settlement approved in 2024.
Dec 2022	**US regulators (HHS OCR)** warn that tracking tools on health websites can disclose PHI.
Feb 2023	**FTC fines GoodRx $1.5M** for sharing health data via pixels; BetterHelp follows with $7.8M in refunds.
Jun 2024	**A federal court strikes down part** of the regulators' warning, for public pages. They drop their appeal.

Where the line is today

Clear violation

Logged-in and booking pages

Pixels on patient portals, booking or symptom forms, and uploading patient lists.

Grey area

Public pages

After the 2024 ruling, a visit plus an IP address isn’t PHI on its own. Lawsuits and state laws still apply.

Not HIPAA

Health apps and brands

Not clinics, so not HIPAA. But the FTC and state laws still punish health-data sharing.

Worth knowing: most pixel cases so far ended in class-action settlements and FTC orders, not HIPAA fines.

4

PART 4 OF 4

Advertising safely

Keep advertising, keep patient data out

4 · ADVERTISING SAFELY

Six ways to advertise safely

01

No Pixel on sensitive pages

Remove it from portals, booking and symptom forms.

02

Go server-side

Send events from your server, so you decide every field.

03

Use a BAA middleman

A tool that signs a BAA strips PHI before anything reaches Meta.

04

Keep bookings off Meta

Track bookings yourself. Send only early, public steps like ad clicks.

05

Broad targeting only

Age, location, interests. Never patient lists or lookalikes.

06

Turn on Core setup

You can enable Meta’s stricter mode yourself in Events Manager.

Three tips from advertisers

Optimize for an earlier step

Choose a goal that happens before any health data.

✓ Goal: link clicks (safest)

~ Goal: public page views (grey area)

✕ Goal: completed bookings

Measure in your own system

Meta can’t see bookings, so count real results in your booking or billing system, not Meta’s reports.

Keep ad wording general

Talk about the topic, not a diagnosis or outcome.

✓ “Learn about managing blood sugar”

✕ “Struggling with your diabetes?”

✓ “Free guide: healthy sleep habits”

✕ “Cure your insomnia in 2 weeks”

Audit checklist for your website

- [x] List every page that has a Pixel
- [x] None on portals, booking or forms
- [x] No conditions in URLs or event names
- [x] Form fields never sent to Meta
- [x] No patient lists uploaded to Meta
- [x] Any middleman has signed a BAA (ex: GoHighLevel)
- [x] Lead forms ask no health questions
- [x] Re-check after every site change

RECAP

Five things to remember

1. Meta won’t sign a BAA. PHI must never reach it.
2. The Pixel sends data by default. Audit where it runs.
3. Hashing isn’t anonymous. Patient lists are off-limits.
4. Public pages are a grey area; logged-in pages are not.
5. Keep bookings off Meta, go server-side, target broadly.

SOURCES

Read more

Quarles: HHS drops tracking appeal
quarles.com › aha-v-becerra

TechTarget: Novant Health settlement
techtarget.com › novant-health

Davis Wright Tremaine: FTC, GoodRx, BetterHelp
dwt.com › ftc-pixel-tracking

Penrod: Meta Ads and HIPAA
penrod.co › meta-ads-and-hipaa

Holland & Knight: court ruling explained
mondaq.com › court dials back OCR bulletin

NatLaw Review: Advocate Aurora settlement
natlawreview.com › advocate-aurora

Search Engine Land: Meta health restrictions
searchengineland.com › meta-ads-restrictions

Freshpaint: HIPAA-safe Facebook ads
freshpaint.io › facebook-ads-hipaa