



FREE EBOOK

The Compliant Healthcare Outreach Handbook

CAN-SPAM, GDPR, CCPA and What HIPAA Does (and Doesn't) Cover

WRITTEN BY

John Britton

VP of Marketing, MedicalProspects

October 2026 Edition
MEDICALPROSPECTS.COM

The Compliant Healthcare Outreach Handbook

CAN-SPAM, GDPR, CCPA and What HIPAA Does (and Doesn't) Cover

ABOUT THIS EBOOK

This MedicalProspects handbook gives healthcare marketing, sales and compliance teams a clear map of the rules that apply to B2B outreach. It explains why HIPAA is usually the wrong question, covers U.S., EU, UK and Canadian email and privacy rules, channel-by-channel requirements and healthcare-specific rules on incentives and promotion, and ends with a workflow and legal sign-off template. It is general guidance, not legal advice.



John Britton
VP of Marketing, MedicalProspects

John works with healthcare sales and marketing teams on precision targeting, campaign strategy, and audience intelligence solutions at MedicalProspects.

October 2026 Edition. © 2026 MedicalProspects, a DataInfoMetrix company. All rights reserved. You may share this ebook in full with attribution; excerpts may be quoted with a link to medicalprospects.com.

This publication is for general information. It is not legal advice; regulations change and vary by jurisdiction, so confirm how they apply to your campaigns with qualified counsel. Statistics are cited to their sources in the Sources section; examples marked illustrative are hypothetical.

MedicalProspects · 7901 4th St N, Ste 300, St. Petersburg, FL 33702 · sales@medicalprospects.com · medicalprospects.com

CONTENTS

What's inside

	INTRODUCTION	3
	Compliance Gets Campaigns Approved	
01	CHAPTER	5
	Professional Data vs. Patient Data, and What HIPAA Covers	
02	CHAPTER	7
	CAN-SPAM in Practice for Healthcare B2B Email	
03	CHAPTER	10
	U.S. State Privacy Laws and B2B Contacts	
04	CHAPTER	12
	International Outreach: GDPR, UK PECR and CASL	
05	CHAPTER	14
	Channel-by-Channel Rules	
06	CHAPTER	16
	Healthcare-Specific Rules: Incentives, Transfers of Value and Promotion	
07	CHAPTER	19
	Building a Compliant Outreach Program	
08	CHAPTER	22
	Pre-Launch Checklist and Legal Sign-Off Template	
09	CHAPTER	25
	Handling Rights Requests and Complaints	
	CONCLUSION	27
	Compliance Starts With the Data	
A	APPENDIX A	29
	Regulation Quick Reference	
B	APPENDIX B	30
	Glossary	
	REFERENCE	31
	Sources	

AT A GLANCE

The short version

This MedicalProspects handbook gives healthcare marketing, sales and compliance teams a clear map of the rules that apply to B2B outreach. It explains why HIPAA is usually the wrong question, covers U.S., EU, UK and Canadian email and privacy rules, channel-by-channel requirements and healthcare-specific rules on incentives and promotion, and ends with a workflow and legal sign-off template. It is general guidance, not legal advice.

KEY TAKEAWAYS

- **HIPAA protects patient data**, not clinicians' professional contact details; the real question is where the data came from.
- **CAN-SPAM's seven requirements** apply to every commercial email, including B2B, with a compliant footer you can adapt.
- **California is the outlier**: since 2023, B2B contacts have full CCPA/CPRA privacy rights.
- **International rules differ**: GDPR legitimate interests, UK PECR corporate subscribers and Canada's CASL consent.
- **Each channel has its own rules**, especially automated calls and texts to mobile numbers.
- **Healthcare-specific rules** on kickbacks, Open Payments, industry codes and FDA promotion shape what outreach can offer and claim.

INTRODUCTION



Compliance Gets Campaigns Approved

Many healthcare campaigns are never stopped by a regulator. They are stopped earlier, by an internal compliance review that cannot get clear answers. The list is bought and the emails are written, then legal asks, "Is this HIPAA-compliant?" and the launch stalls for weeks.

IN THIS CHAPTER

- How to use this handbook

Most of these delays come from a few misunderstandings. HIPAA is usually the wrong question. CAN-SPAM is simpler than people fear. The rules that most often catch healthcare marketers out are elsewhere: state privacy laws, international consent rules, phone and text rules, and healthcare-specific rules on gifts and promotion.

This handbook is for healthcare marketing, sales and compliance teams who want a clear, practical map:

- **What HIPAA covers**, and why professional contact data is a different matter
- **The U.S. email, privacy and phone rules** that apply to B2B healthcare outreach
- **International rules** for reaching providers in the EU, UK and Canada
- **Healthcare-specific rules** on incentives, transfers of value and promotional content
- **A step-by-step compliant outreach workflow**, a pre-launch checklist and a sign-off template for legal review

I NOT LEGAL ADVICE

This handbook is general guidance. Laws change and differ by jurisdiction. Have qualified counsel confirm how they apply to your company, products and campaigns.

\$53,088

maximum penalty per email that violates CAN-SPAM

FTC¹

10 days

business days to honor an opt-out

FTC¹

0.3%

spam-rate ceiling Gmail sets for bulk senders

Google sender guidelines²

4%

of worldwide turnover, the GDPR maximum fine (or €20M if higher)

GDPR Art. 83³

Those four numbers set the stakes. Penalties apply per message, mailbox providers act on complaint rates before any regulator does, and the largest fines are tied to revenue. Compliance is cheaper to build in than to fix later.

How to use this handbook

Read chapters 1 to 6 once as a team, then use chapters 7 and 8 and the appendices every time you launch a campaign. Chapter 9 explains how to handle rights requests and complaints.

KEY TAKEAWAYS

- HIPAA protects patient information, not professionals' business contact details.
- The real questions are lawful sourcing and compliant messaging.
- Get a written statement from your list vendor that no data comes from patient records.

Professional Data vs. Patient Data, and What HIPAA Covers

HIPAA protects patients' health information. It does not govern the business contact details of the clinicians who treat them. Getting this distinction clear removes the most common blocker in healthcare list purchases.

IN THIS CHAPTER

- What HIPAA protects
- Why professional contact data is different
- Where HIPAA does matter for marketers

What HIPAA protects

HIPAA's Privacy Rule protects **protected health information (PHI)**: individually identifiable health information about patients held by **covered entities** (health plans, clearinghouses and most providers) and their **business associates**.

Why professional contact data is different

Data	Whose information	Is it PHI?
A cardiologist's business email and practice address	The clinician's, as a professional	No
A physician's NPI, specialty and hospital affiliation	The clinician's, much of it published by CMS	No
A hospital CIO's direct dial and title	The executive's, as a professional	No

Data	Whose information	Is it PHI?
A list of patients seen by a cardiologist	Patients'	Yes
Diagnoses, appointments or prescriptions tied to patients	Patients'	Yes

Where HIPAA does matter for marketers

- **Data sources.** Confirm in writing that your list vendor never sources contacts from patient records, clinical systems or covered entities' patient data.
- **Patient-facing campaigns.** If your company is a covered entity or business associate and markets to patients, HIPAA's marketing rules apply. That is outside this B2B handbook.
- **What you ask for in replies.** Do not invite clinicians to send patient details by email in response to your outreach.

Bottom line: For B2B outreach to healthcare professionals, the question is not "Is this HIPAA-compliant?" It is "Was this data sourced lawfully, and do our messages follow the email, privacy and healthcare promotion rules?" The rest of this handbook answers that question.

KEY TAKEAWAYS

- CAN-SPAM has no B2B exemption, but it does not require prior consent.
- Seven requirements cover almost every mistake, from honest headers to monitoring your agents.
- Build the footer and opt-out sync into templates and tools, not individual campaigns.

CAN-SPAM in Practice for Healthcare B2B Email

CAN-SPAM lets you email U.S. healthcare professionals without prior consent, as long as every message follows its rules. There is no B2B exemption: the rules apply to every commercial email, including those sent to work addresses.

IN THIS CHAPTER

- The seven requirements
- Why it matters
- A compliant footer you can adapt
- Gmail and Yahoo rules sit on top of CAN-SPAM
- Common healthcare mistakes

The seven requirements

Requirement	What it means in a healthcare campaign
1. Accurate header information	"From", "Reply-To" and the sending domain identify your company. No borrowing a partner's or a hospital's name.
2. Honest subject lines	The subject reflects the content. "Re: your patient referral" on a sales email is deceptive.
3. Identify the message as an ad	Make clear the email is commercial. Plain, professional wording is enough.
4. A valid physical postal address	A street address, a registered P.O. box or a registered private mailbox in every email.
5. A clear way to opt out	A visible unsubscribe link or reply method that works for at least 30 days after sending. ¹

Requirement	What it means in a healthcare campaign
6. Honor opt-outs within 10 business days	No fee, no login and no more than a reply or one web page to opt out. Never sell or share opted-out addresses.
7. Monitor others acting for you	You stay responsible when an agency or platform sends on your behalf.

Why it matters

Each non-compliant email can bring a civil penalty of up to \$53,088 under FTC rules.¹ Volume campaigns multiply that risk quickly, so build these rules into your templates rather than checking each send.

A compliant footer you can adapt

[Company legal name] · [Street address, City, State ZIP]

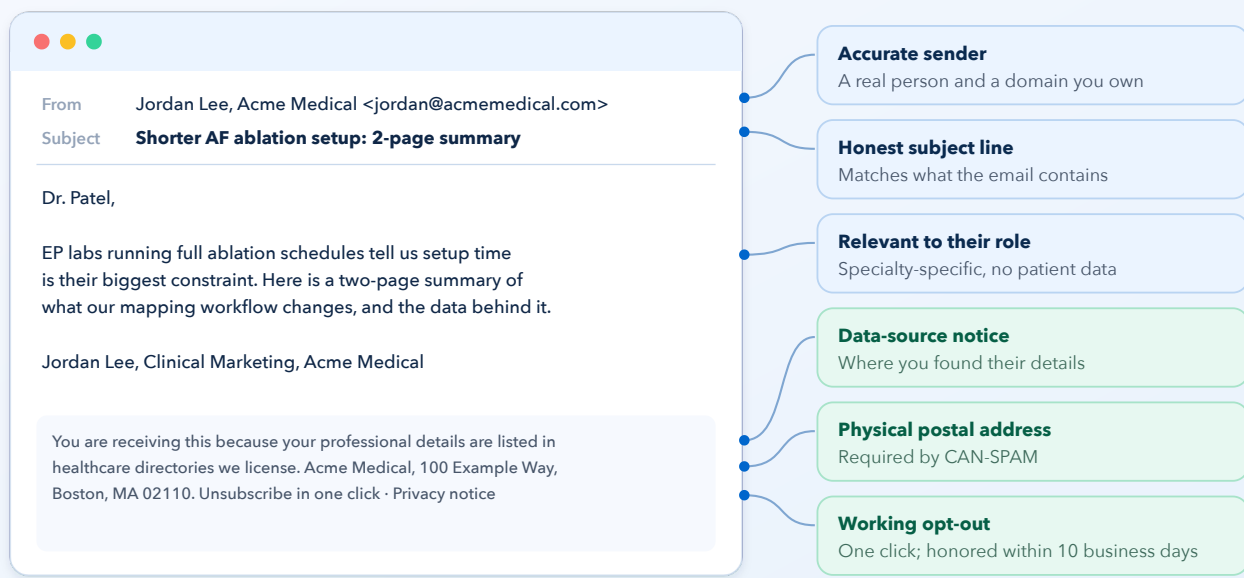
You are receiving this email because your professional role relates to [product area].
We found your business contact details in public professional sources and registries.
To stop receiving these emails, [unsubscribe here] or reply "unsubscribe".

A COMPLIANT FIRST-TOUCH EMAIL, ANNOTATED (ILLUSTRATIVE)

The figure below shows a short email to an electrophysiologist with each required element marked: a real sender, an honest subject, a data-source notice, a postal address and a working one-click opt-out.

Anatomy of a compliant first-touch email

Illustrative example; names and addresses are fictitious



Anatomy of a compliant first-touch email, with each required element marked

Gmail and Yahoo rules sit on top of CAN-SPAM

Mailbox providers now enforce sender requirements of their own. Google's guidelines ask senders to authenticate mail (SPF, DKIM and DMARC), support one-click unsubscribe for marketing messages and keep spam rates below 0.3%, ideally below 0.10%. Senders who send more than 5,000 messages a day to Gmail accounts face the strictest requirements.² A campaign can be legal under CAN-SPAM and still land in spam if it breaks these rules.

Common healthcare mistakes

- Sending from a lookalike or rented domain that hides who you are
- Opt-outs held in one tool but not shared with the SDR sequencing platform
- Subject lines that imply an existing clinical relationship ("Following up on your patient")
- Agencies running campaigns under your brand without your suppression list

KEY TAKEAWAYS

- California treats business contacts like consumers; plan for access, deletion and opt-out requests.
- Most other state laws still exclude business-context data, but the list keeps changing.
- Pass deletion requests to your vendor and every tool that holds the record.

U.S. State Privacy Laws and B2B Contacts

California is the state that changes the picture for B2B healthcare data. Since January 1, 2023, when the employee and B2B exemptions expired, the CCPA, as amended by the CPRA, has given business contacts the same privacy rights as consumers.⁴ Most other state privacy laws still exclude people acting in a business or employment role.

IN THIS CHAPTER

- California (CCPA / CPRA)
- What to do
- Other states

California (CCPA / CPRA)

If your company meets the CCPA's thresholds, California-based clinicians and executives on your lists have the right to:

- **Know** what personal information you hold about them and where it came from
- **Delete** that information, subject to limited exceptions
- **Correct** inaccurate information
- **Opt out** of the sale or sharing of their information
- **Not be discriminated against** for using these rights

California also regulates **data brokers**, the companies that sell data about people they have no direct relationship with. Data brokers must register with the state and process deletion requests made through the state's central deletion system. Ask whether your list vendor is registered where required.

Other states

Comprehensive privacy laws in states such as Virginia, Colorado, Connecticut and Texas generally exclude information about people acting in a commercial or employment context. That usually takes B2B professional contacts out of scope, but the details differ by state and keep changing.

What to do

- ☐ Confirm with counsel whether your company meets the CCPA thresholds
- ☐ Update your privacy notice to cover prospect data and where it comes from
- ☐ Set up a process to answer access, deletion and correction requests
- ☐ Pass deletion requests to your list vendor and every tool that holds the record
- ☐ Review new state laws each quarter, as several are added every year

KEY TAKEAWAYS

- Consent rules differ by country; segment lists and apply each market's rules.
- GDPR B2B outreach usually relies on legitimate interests, with a documented assessment and a data-source notice.
- Where consent is required, start with channels that do not need it, such as direct mail.

International Outreach: GDPR, UK PECR and CASL

Outside the U.S., the key question is whether you need consent before the first email. The answer differs by country, so plan each market separately.

IN THIS CHAPTER

- At a glance
- GDPR (EU and UK)
- UK PECR
- Canada's CASL
- Practical rules for global campaigns

At a glance

Market	Main rules	Consent before a B2B email?	Key obligations
European Union	GDPR + national ePrivacy laws	Varies by country; some (e.g., Germany) effectively require it	Lawful basis, notice of data source, rights requests answered within one month
United Kingdom	UK GDPR + PECR	Not for corporate addresses; yes for sole traders and some partnerships	Opt-out in every message, notice of data source
Canada	CASL + PIPEDA	Yes, express or implied	Sender identification, working unsubscribe, consent records

GDPR (EU and UK)

- **Lawful basis.** B2B outreach usually relies on **legitimate interests** (Article 6(1)(f)). Document a Legitimate Interests Assessment showing your outreach is relevant to the person's role and proportionate.
- **Tell people where you got their data.** When data comes from a third party, Article 14 requires you to give the person a privacy notice, at the latest in your first communication and within one month.
- **Respect rights.** Access, deletion and objection requests must be answered within one month. An objection to direct marketing must always be honored.
- **Penalties.** Serious breaches can bring fines of up to €20 million or 4% of global annual turnover, whichever is higher.³

UK PECR

You can send B2B marketing email to **corporate subscribers**, such as staff at an NHS trust or a limited company, without prior consent, if you identify yourself and offer an opt-out. **Individual subscribers**, such as sole traders and some partnerships, need prior consent. Many independent practitioners fall into this group.

Canada's CASL

CASL requires consent before you send a commercial electronic message. **Implied consent** can apply when a professional has published their business email openly, the message relates to their role, and they have not said they do not want unsolicited messages. Keep records showing how consent applied to each contact.

Practical rules for global campaigns

- Segment lists by country and apply each country's rules
- Put a short data-source notice and privacy link in every first-touch email
- Keep consent and legitimate-interest records with each contact
- When in doubt, start with channels that need no consent, such as direct mail, and invite people to opt in

KEY TAKEAWAYS

- Each channel has its own rules: a contact you may email may still need consent before you text.
- Treat mobile numbers carefully; many "direct dials" are personal mobiles.
- Keep one source of truth for opt-outs across every channel and partner.

Channel-by-Channel Rules

Each outreach channel has its own rules. A contact you may email freely may still need consent before you text them. Check the channel rules before you build a multi-channel sequence.

IN THIS CHAPTER

- Mobile numbers deserve extra care
- Keep one source of truth for opt-outs

Channel	Main U.S. rules	Consent needed?	Watch out for
Email	CAN-SPAM	No, but opt-out required	Opt-outs not synced across tools
Phone, manual dialing to business lines	TCPA, state telemarketing laws	Generally no	Calling hours, state registration rules
Phone, autodialed or prerecorded to mobiles	TCPA	Yes, prior express written consent for marketing	Many "direct dials" are personal mobile numbers
SMS / text	TCPA, state laws such as Florida's FTSA	Yes, prior express written consent	Automated texting platforms count as autodialing in many cases
Fax	Junk Fax Prevention Act	Established business relationship + opt-out notice	Fax is still common in healthcare, and unsolicited fax ads draw lawsuits
Direct mail	Postal rules; privacy laws cover the data	No	Honor do-not-mail requests
LinkedIn	LinkedIn User Agreement	Platform rules apply	Scraping and automation tools break the terms

Mobile numbers deserve extra care

The TCPA treats calls and texts to mobile phones more strictly than calls to landlines, even when the phone is used for work. Before any automated dialing or texting:

- ☐ Identify which numbers are mobile
- ☐ Scrub against the National Do Not Call Registry and your internal do-not-call list
- ☐ Use manual dialing unless you hold prior express written consent
- ☐ Check state rules in the states you are calling

Keep one source of truth for opt-outs

An opt-out from any channel should follow the contact everywhere. Sync email unsubscribes, do-not-call requests and deletion requests across your CRM, sequencing tool, dialer and agency partners.

KEY TAKEAWAYS

- The biggest healthcare risk is what an email offers or claims, not the email itself.
- Avoid gifts and prizes for clinicians who prescribe, order or refer; use educational value.
- Route promotional content through medical, legal and regulatory review first.

Healthcare-Specific Rules: Incentives, Transfers of Value and Promotion

Healthcare outreach carries risks that general B2B guides ignore. The biggest is not the email itself but what the email offers and claims. A \$50 gift card for booking a demo is routine in SaaS marketing. Offered to a prescribing physician, it can create legal and reporting obligations.

IN THIS CHAPTER

- Which rules apply to whom
- Promotional content
- Incentives in campaigns

Which rules apply to whom

Rule	Applies to	What it means for outreach
Federal Anti-Kickback Statute	Anyone whose products or services are paid for by Medicare, Medicaid or other federal health programs	Do not offer anything of value to induce clinicians to order, prescribe or refer your products
Open Payments (Physician Payments Sunshine Act)	Manufacturers of covered drugs, devices, biologicals and supplies, and group purchasing organizations	Payments and transfers of value to physicians, teaching hospitals, PAs and nurse practitioners must be reported to CMS
PhRMA Code	Pharmaceutical companies (voluntary industry code)	Strict limits on meals and gifts; no non-educational items

Rule	Applies to	What it means for outreach
AdvaMed Code	Medical device companies (voluntary industry code)	Similar limits on gifts, meals and entertainment for HCPs
State gift and disclosure laws	Manufacturers selling in states such as Vermont, Minnesota and Massachusetts	Extra gift bans or disclosure duties beyond federal rules
FDA promotion rules	Prescription drug, biologic and device marketers	Claims must be truthful, balanced and within approved or cleared uses
FTC Act	Every company, including HealthTech and services	Claims must be truthful and backed by evidence

Incentives in campaigns

- **Avoid gift cards, cash or prizes** for clinicians who prescribe, order or refer your products. Use educational value instead, such as research summaries, CME-eligible events run by accredited providers, or clinical tools.
- **Track every transfer of value.** Meals at events, travel and fees for advisory work may be reportable under Open Payments. Capture the recipient's NPI so reports match CMS records.
- **Check the recipient type.** Rules can differ for physicians, nurse practitioners, hospital executives and IT buyers. Your compliance team should set clear rules for each audience.

Promotional content

- **Prescription drugs and biologics:** promotional emails need fair balance and important safety information. Materials are generally submitted to FDA (Form FDA 2253) when first used.
- **Medical devices:** keep claims within cleared or approved indications. Do not promote off-label uses in outreach.
- **HealthTech and services:** back every outcome claim, such as "reduces readmissions by 20%", with evidence you can produce.

Always route healthcare promotional content through your company's medical, legal and regulatory (MLR) review before it reaches a clinician's inbox.

WORKSHEET · MAP YOUR CONSENT DECISIONS

Complete one line for each market and channel you use.

1. Markets you contact (U.S. states, EU countries, UK, Canada):

2. Channels used in each market:

3. Where prior consent is required, and how you obtain and record it:

4. Where you rely on legitimate interests, and where the assessment is stored:

Building a Compliant Outreach Program

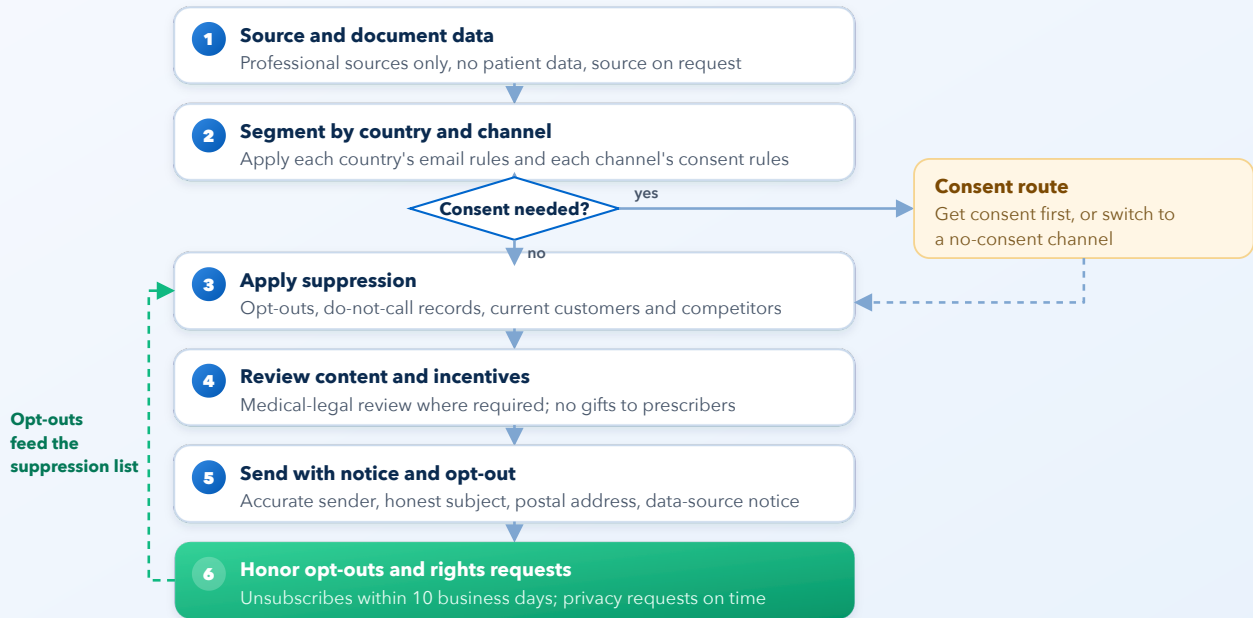
Compliance holds up when it is built into the workflow rather than checked campaign by campaign. Every campaign follows the same six steps. The step that matters most is the last one: every opt-out and rights request flows back into the suppression list before the next send.

IN THIS CHAPTER

- What a documented program looks like
- Who owns each step

Compliant outreach workflow

Six steps, one consent decision and one feedback loop



Compliant outreach workflow: six steps, one consent decision and one feedback loop

The consent decision happens once per country and channel, not per contact. Most U.S. email and manual calling needs no prior consent. Automated calls or texts to mobiles, Canadian email and some EU markets do.

What a documented program looks like

Reviewers and customers increasingly ask to see how you work, not just what you promise. A short compliance file for your outreach program usually includes:

- Your data sourcing statements from each vendor
- A map of markets, channels and the consent basis for each
- Your suppression-list process and sync schedule
- Your content-review procedure and approver names
- A log of rights requests, with response dates
- A copy of each approved campaign sign-off

Who owns each step

Step	Typical owner	Record to keep
1. Source and document data	Marketing operations	Vendor sourcing statement and data agreement
2. Segment by country and channel	Marketing operations	Country and channel rules applied per segment
3. Apply suppression	Marketing operations	Suppression list version and date
4. Review content and incentives	Compliance / MLR	Approval record and reviewer
5. Send with notice and opt-out	Demand generation / sales development	Final template and send log
6. Honor opt-outs and rights requests	Privacy owner	Request log with response dates

KEY TAKEAWAYS

- Build compliance into the six-step workflow so every campaign follows it.
- Assign an owner and a record to each step.
- The step that closes the loop, honoring opt-outs, is the one most programs skip.

★ MAKE THE OPT-OUT EASY

A clear, one-step unsubscribe satisfies the rules and keeps unhappy recipients from marking your email as spam, which hurts deliverability for everyone else on the list.

Pre-Launch Checklist and Legal Sign-Off Template

Run this checklist before every new campaign. Then send the sign-off template to your legal or compliance reviewer, filled in, so they can approve the campaign in one pass instead of over weeks of email.

IN THIS CHAPTER

■ Pre-launch checklist

■ Legal sign-off template

Pre-launch checklist

Data

- ☐ Vendor has confirmed in writing that no data comes from patient records
- ☐ Data sources are documented and available if a contact asks
- ☐ Contacts are segmented by country, and each country's rules are applied
- ☐ Current customers, opt-outs and do-not-contact records are suppressed

Email

- ☐ Sending domain and "From" name identify your company
- ☐ Subject lines match the content
- ☐ Physical postal address and a working unsubscribe link are in every email
- ☐ Data-source notice and privacy link are in first-touch emails

Phone and text

- ☐ Mobile numbers identified, with manual dialing unless consent is on file

- ☐ Numbers scrubbed against the National Do Not Call Registry and internal lists

Content and incentives

- ☐ Content passed medical, legal and regulatory (MLR) review where required
- ☐ No gifts or incentives to clinicians who prescribe, order or refer your products
- ☐ Transfers of value tracked with recipient NPIs for Open Payments

Rights and records

- ☐ Access, deletion and objection requests have an owner and a deadline
- ☐ Opt-outs sync across CRM, sequencing tool, dialer and agencies

Legal sign-off template

OUTREACH CAMPAIGN COMPLIANCE SIGN-OFF

Campaign: [name] Owner: [name] Launch date: [date]

AUDIENCE

Roles / specialties: [e.g., interventional cardiologists, hospital CIOs]

Countries and U.S. states: [list]

Volume: [number of contacts]

Data vendor and sources: [vendor; source types]

CHANNELS

☐ Email ☐ Manual phone ☐ Automated phone/SMS (consent on file?)

☐ Direct mail ☐ LinkedIn ☐ Fax

CONTENT

Product type: [Rx drug / device / HealthTech / service]

MLR review completed: [yes / not required, with reason]

Incentives or items of value offered: [none / describe]

CONTROLS

Suppression list applied: [yes, date]

Unsubscribe and postal address in template: [yes]

Data-source notice included: [yes]

GDPR legitimate interests assessment (if EU/UK): [link]

APPROVAL

Reviewer: [name] Decision: [approved / approved with changes / rejected] Date: [date]

KEY TAKEAWAYS

- Run the pre-launch checklist before every campaign.
- Send legal one filled-in sign-off page, not weeks of email.
- Keep the evidence: sources, assessments, approvals and request logs.

Handling Rights Requests and Complaints

Sooner or later a recipient will ask where you got their data, ask you to delete it or complain to a regulator or your vendor. A prepared response keeps a small request from becoming a large problem.

IN THIS CHAPTER

- A simple response process
- Handling an angry reply

A simple response process

Step	What to do	Typical deadline
1. Log the request	Record who asked, what they asked and when it arrived	Same day
2. Verify the person	Confirm the request is genuine before acting	A few days
3. Find the data	Search your CRM, sequencing tool, dialer, spreadsheets and agency files	Within the legal deadline
4. Act	Delete, correct, export or stop processing, as requested	One month under GDPR
5. Notify others	Tell your vendor and any partners that hold the record	Same time as step 4
6. Respond and record	Confirm what you did, and keep a record	Within the legal deadline

Handling an angry reply

Most complaints come from recipients who feel the email was irrelevant or that they never agreed to hear from you. Respond politely, remove them from every list at once and tell them where their details came from. A fast, courteous answer ends most complaints.

DO NOT KEEP EMAILING SOMEONE WHO HAS OPTED OUT

Sending even one more message after an opt-out is the fastest way to turn a minor complaint into a violation. Sync suppression across every tool before the next send.

KEY TAKEAWAYS

- Log, verify, find, act, notify and respond; give every request an owner and a deadline.
- Search every tool and partner that holds the record.
- Answer complaints quickly and politely, and suppress the person everywhere.

CONCLUSION



Compliance Starts With the Data

Compliant outreach starts before the first email is written, with where the contact data comes from and how it is maintained. With a clean, documented source, the remaining rules come down to habits: honest messages, working opt-outs, the right channel for each contact, and incentives your compliance team can defend.

IN THIS CHAPTER

- How MedicalProspects supports compliant outreach
- Start with a sample

How MedicalProspects supports compliant outreach

Your requirement	How MedicalProspects helps
Lawful, documented sources	Records compiled from professional sources such as the CMS NPI registry, licensing boards, medical association directories and licensed B2B partners
No patient data	Never sourced from patient health records or clinical systems
Accurate records	Monthly re-verification, with 60-day cycles for high-turnover roles, and retired or deactivated providers removed
Rights requests	Access, correction and deletion requests answered within 30 days via privacy@medicalprospects.com
GDPR alignment	EU and UK professional data processed under legitimate interests (Article 6(1)(f))

Your requirement	How MedicalProspects helps
Secure delivery	Data encrypted in transit (TLS 1.3) and at rest (AES-256)
NPI on clinical records	Supports Open Payments tracking and suppression by NPI

Start with a sample

Request 20 free custom sample contacts built on your criteria. Share them with your compliance team along with this handbook's checklist, and see how quickly a campaign can be approved when the data is documented from the start.

Visit medicalprospects.com or email sales@medicalprospects.com.

APPENDIX A



Regulation Quick Reference

Rule	Where	Applies to	Core requirement
CAN-SPAM	U.S.	Commercial email	Honest headers, postal address, working opt-out, honor opt-outs within 10 business days
TCPA	U.S.	Calls and texts	Consent for autodialed or prerecorded calls and texts to mobiles
CCPA / CPRA	California	Personal information, including business contacts	Notice, access, deletion, correction and opt-out rights
GDPR	EU	Personal data of EU residents	Lawful basis, source notice, rights handled within one month
UK GDPR and PECR	UK	Personal data and electronic marketing	Corporate subscribers need no consent; individuals do
CASL	Canada	Commercial electronic messages	Express or implied consent, sender ID, unsubscribe
Anti-Kickback Statute	U.S.	Federal health program payors and suppliers	Nothing of value to induce orders, prescriptions or referrals
Open Payments	U.S.	Drug, device and biologic manufacturers	Report transfers of value to physicians and certain other clinicians

APPENDIX B



Glossary

Term	Meaning
PHI	Protected health information: individually identifiable patient health information under HIPAA
Covered entity	A health plan, clearinghouse or provider covered by HIPAA
Business associate	A company that handles PHI on behalf of a covered entity
Legitimate interests	A GDPR lawful basis often used for relevant B2B outreach
Suppression list	Contacts you must not email, call or text
MLR review	Medical, legal and regulatory review of promotional content
Open Payments	CMS program that publishes manufacturers' payments to physicians and teaching hospitals
TCPA	Telephone Consumer Protection Act, governing calls and texts
Data broker	A company that sells personal data about people it has no direct relationship with
NPI	National Provider Identifier: the unique 10-digit identifier for U.S. health care providers

REFERENCE

Sources

1. Federal Trade Commission, CAN-SPAM Act: A Compliance Guide for Business. <https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business>
2. Google Workspace Admin Help, Email sender guidelines. <https://support.google.com/a/answer/81126>
3. General Data Protection Regulation, Article 83(5). <https://gdpr-info.eu/art-83-gdpr/>
4. Morgan Lewis, California Consumer Privacy Act employee and B2B exemptions expire January 1, 2023. <https://www.morganlewis.com/pubs/2022/10/california-consumer-privacy-act-employee-and-b2b-exemptions-expire-january-1-2023>

ABOUT THE AUTHOR



John Britton

VP of Marketing, MedicalProspects

John works with healthcare sales and marketing teams on precision targeting, campaign strategy, and audience intelligence solutions at MedicalProspects.

ABOUT MEDICALPROSPECTS

MedicalProspects provides verified healthcare contact data for B2B marketing and sales teams: 425+ specialty, role and facility lists anchored to NPI and NUCC taxonomy data, re-verified monthly, with technology and buying-intent intelligence available on every audience. Teams use it to reach physicians, nurses, hospital executives, IT leaders, life sciences and payer decision-makers.

Get 20 free sample contacts built on your criteria.

medicalprospects.com · sales@medicalprospects.com



NEXT STEP

See the difference verified data makes

Get 20 free sample contacts built on your exact targeting criteria. Check them with your own tools before you buy anything.

15.17M+

unique verified healthcare contacts

425+

specialty, role and facility lists

99%

deliverability guarantee, 1:1 bounce replacement

24-48h

delivery, re-verified monthly

Request your free sample at **medicalprospects.com**

eBook 04 • MedicalProspects GTM Library

sales@medicalprospects.com • +1 727-617-0017 • 7901 4th St N, Ste 300, St. Petersburg, FL 33702

© 2026 MedicalProspects, a DataInfoMetrix company. For B2B professional outreach only.