www.getdeardoc.com

HIPAA-Compliant Marketing Guide

Tactics, Expert Tips, and Checklists

DearDoc

Introduction

Much of modern marketing relies on customer engagement. From testimonials and reviews to social media where followers can comment and message your business.

But in the healthcare industry, you have the added hurdle of making sure that everything you do to promote your practice is HIPAA-compliant.

So how do you interact with patients through different marketing channels while protecting your patients' identity and protected health information?

We will cover all of the above in this guide, including expert tips from Compliancy Group.

Grow Your Practice with Expert Tools

DearDoc offers cloud-based software solutions including a HIPAA-compliant AI Chatbot that's trusted by 2,500+ healthcare systems to modernize how doctors interact with new and existing patients.

Book a personalized demo and learn more today:

BOOK DEMO

Components of a HIPAA Compliant Marketing Plan

1. Business Associate Contracts

HIPAA regulations include health care businesses (as covered entities), as well as anyone they work with to run their business (as business associates).

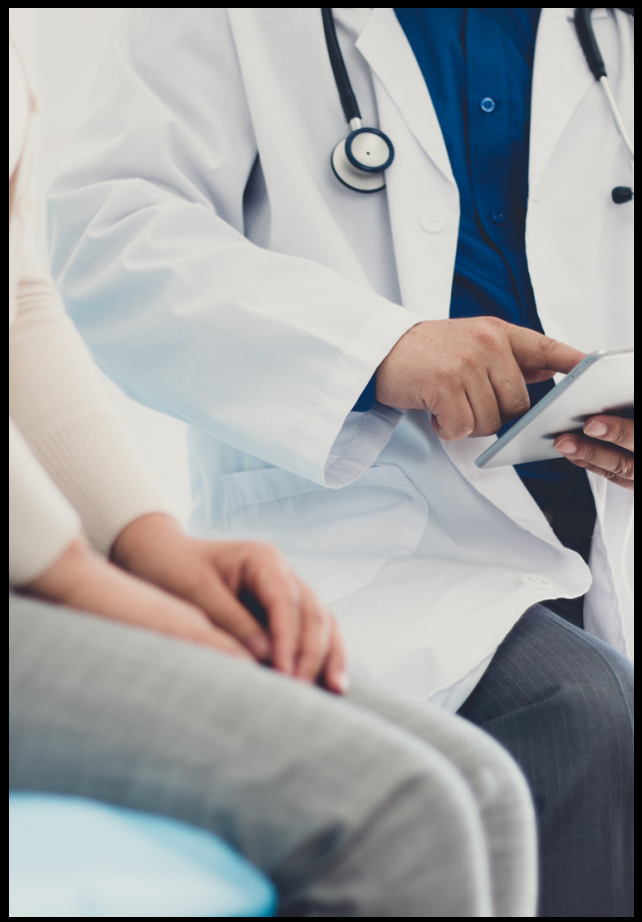
If you're using any external solutions, agencies, or contractors to connect to patients or promote your practice, you need to have a contract in place with them about their responsibilities to stay HIPAA compliant.

A Business Associate Contract is a legal agreement in which both parties acknowledge they fall under HIPAA's rules and are each individually responsible to stay compliant.

> A business associate agreement creates a firewall between you and the vendor you're working so that, if your vendor ever has an issue from a HIPAA perspective, that can't come back to haunt you. And vice versa, if you ever have an issue, it will not impact the vendor you're working with.
>
> - Compliancy Group

Key Takeaway

Make sure you have a Business Associate Contract in place with any third-party vendors you're using.



2. Patient Consent Forms

A physical therapy practice was fined $25,000 for posting patients' names and photos on the testimonials section of their website without first collecting HIPAA-compliant authorization forms.

Even though what was posted was positive experiences from patients, the individuals who emailed or wrote the practice about their experience did not necessarily agree to have them shared publicly. And even if they did agree, the practice did not have the forms in place to protect their practice from a complaint.

Written consent is needed to disclose any PHI publicly, even if a patient has verbally agreed to you sharing information.

The other necessary authorization is an electronic communication consent form, which gives you permission to email or text your patients.

FAQ

Do you need a consent form to collect personal information from a questionnaire on a website?

If the form potentially collects any PHI, you need some sort of electronic consent, even if it's as simple as a check box that a patient fills in on the form itself.

Key Takeaway

All patients should sign an electronic communication consent form. And before you share any information on your website or social media platforms, the patient needs to sign an authorization form giving their written consent to have aspects of their PHI shared publicly.

For you to be able to email or text your patients,, you need an electronic consent form in place. That, along with any other disclosures and authorization forms, should be one of the first things that the patient signs once they walk into the practice.

- Compliancy Group

3. Privacy Notices

HIPAA Privacy Rule requires health care providers to distribute a notice to individuals about their rights regarding their public health information, as well as the privacy practices of the organization. But you are also required to make this privacy notice available on your website.

Key Takeaway

Make sure your privacy notice is posted prominently on your website.

HIPAA Compliant Marketing Tactics

1. Online Reviews

- **Keep replies to reviews anonymous**

In 2016, a dental practice was fined $10,000 for revealing private health information online when responding to a review that a patient had left on Yelp.

After a bad experience at the practice, the patient left a one-star review which the practice publicly responded to. In the response, the practice included the patient's last name, as well as other details about their treatment and the cost involved. The patient issued a complaint to the Department of Health and Human Services' Office for Civil Rights (OCR).

But when OCR investigated the claim, the resulting fine wasn't for the incident alone. The real issue was that the practice didn't have policies and procedures in place around protected health information (PHI) on social media and other public platforms.

To stay HIPAA-compliant, your response needs to be as anonymous as possible. Even if a patient uses their name or reveals other protected health information, it does not give you the go-ahead to confirm any of this information. In fact, you shouldn't confirm that they are a patient at all.

Keep responses as brief as possible and attempt to take any complaint offline.

We recommend a blanket statement, such as, "We appreciate your feedback. Please call the office so we can address your concerns." Or "Thank you for leaving a review! We care about our patients' overall experience."

- **Do not respond to content posted elsewhere**

If patient posts about their experience somewhere other than an official review platform — for instance, if they tag your practice on Facebook or on their blog — you are better off not responding at all.

By responding, you run the risk of confirming they are a patient, which could be a compliance violation. They are allowed to share whatever personal health data they'd like about themselves. But you're not allowed to confirm any of it without their written consent.

- **Do not alter content when posting reviews or testimonials**

Even if you receive written permission to post a review or testimonial online, you cannot alter any of the content, which could misrepresent the patient. Post any testimonial "as is" to your website or social media account or make sure to have a written log of anything you request to add or change. This includes pictures of the patient.

FAQ

Do I need written authorization for patients to show pictures of a patient when I'm not showing their face at all or only showing a piece of their face like their teeth?

You need written permission if it's a body part that could identify an individual. In general, it's always safer to have the proper authorizations in place anytime you use an image of a specific patient.

2. Social Media

Don'ts

- DO NOT post images and videos of patients without consent
- DO NOT post any information that could allow a patient to be identified
- DO NOT share patient photographs or images taken inside a healthcare facility
- Do NOT alter content
- Do NOT respond to patients sharing of a diagnosis or service
- Do not engage in social media discussions with patients who have disclosed PHI on social media.

Dos

- Train all staff on violations and acceptable uses of patient information for social media or website
- Thank patients for their feedback
- Keep responses anonymous
- Take complaints offline – please call the office
- Focus on the positive when interacting with patients
- Have written consent if you use a patient testimonial

What about messaging patients using Facebook Chat?

According to HIPAA Journal, “without a [business associate agreement] and without appropriate audit and access controls, we do not believe Facebook Messenger is HIPAA compliant.” If you share PHI in Facebook Messenger, you may not be protected in a compliancy review. We recommend sticking with chat tools specifically designed for the healthcare industry.

3. Email Marketing

Due to HIPAA regulations, all healthcare marketing emails are bound by law and cannot display a patient's private information:

- Private information is defined as:
- Demographic information (birth dates, gender, ethnicity)
- Contact and emergency information
- Diagnoses
- Treatment information
- Medical test results
- Prescription information

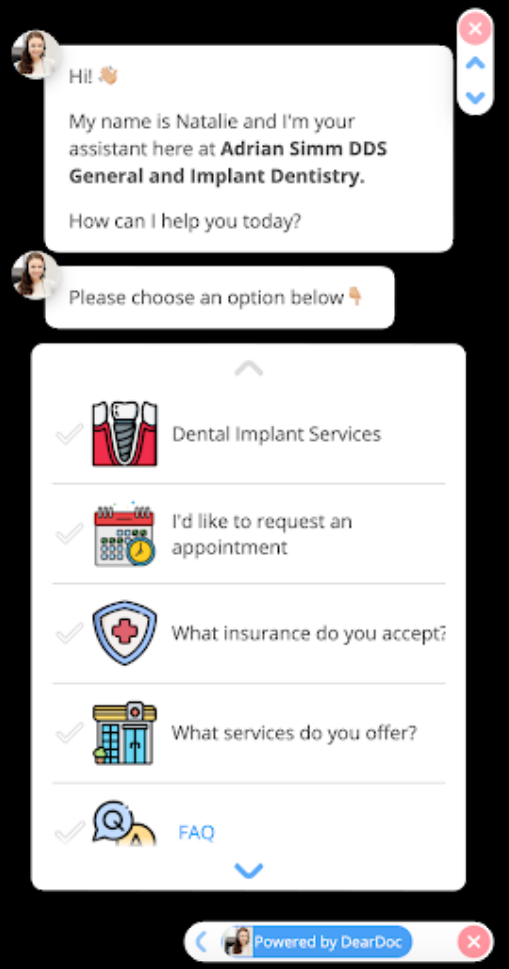
Some considerations to keep in mind as you send out emails to existing or potential patients:

- Send emails to groups of patients with undisclosed recipients. You can do this by simply inputting emails on the BBC. BBC stands for Blind Carbon Copy which makes it impossible to see the entire list of recipients.
- Avoid including personal information in the email. Never send emails about diagnosis, treatment, or other identifying information.
- When it comes to addressing the email, it may be a good idea to avoid using the patient's name. Instead, simply create an email with a generic greeting such as a simple hello.

4. Website

Your practice's website also needs to be HIPAA-compliant, and that includes all the information, testimonial, and chat tools on your website. Here is a HIPAA-compliant website checklist:

- Have a valid SSL certificate
- Use HIPAA- Compliant website forms
- Use HIPAA- Compliant website hosting service
- Get your website and practice certified and post a compliance seal on your website
- Obtain patient consent before publishing their testimonial



DearDoc's HIPAA-Compliant AI Chatbot is designed specifically for healthcare practices to communicate with patients easier online. To free up your admin time and to give your patients a shorter wait time, you can customize common FAQs, insurance information, services offered, and appointment booking using the chat. Book a free demo to see how it can transform your practice's website experience:

BOOK DEMO

Conclusion

> Healthcare is becoming more of a consumer-type environment. If you're not providing these services to patients, many of them are going to look for other practices where they can receive the experience they're looking for.
>
> - Compliancy Group

As patients are becoming increasingly digitalized, healthcare practices need to put more emphasis on building a stronger online presence and a better patient experience. Now more then ever, you need the right tools to transform your patients' online experience without violating compliance rules.

That's why DearDoc's HIPAA-compliant AI Chatbot is trusted by more than 2,500 practices in the nation to connect with patients anytime and anywhere. DearDoc's AI Chatbot also integrates with WebMD and Vitals.com to enable direct patient-to-practitioner communication on your listing. Book a free demo now to learn how it can help your practice:

BOOK DEMO

DearDoc

DearDoc offers cloud-based software solutions to help reinvent the way new patients meet their doctor. We are changing the standard of how patients get in touch with healthcare professionals by offering a selection of advanced tools to modernize how doctors interact with new and existing patients.

For More Information

Click here to find out more >>

(646) 751-8317

75 Broad Street,
New York, New York