Make Sure You Have A HIPAA Compliant Relationship with Your Medical and Dental Practices Marketing Agency

Carl White
MarketVisory Group, Inc
www.marketvisorygroup.com
NSCHBC Member

Many healthcare providers outsource some or all of their marketing to marketing agencies. We find that few of those healthcare providers set up a HIPAA compliant relationship before sharing PHI. Those who do so are putting themselves at unnecessary and avoidable risk.

The goal of this article is to raise your awareness about HIPAA compliance with your marketing agency; an important topic that many healthcare providers do not recognize.

Note

We are a HIPAA compliant healthcare marketing agency. We are not attorneys. You should consult a qualified healthcare attorney for any legal specific questions you may have. There are many qualified healthcare attorneys that are members of NSCHBC.

You Are a Covered Entity According To HIPAA

You have to safeguard protected health information (PHI) and make sure that only authorized people in outside agencies can see it. Under HIPAA you are able to share PHI with outside agencies, which are known as “business associates” as long as you do so in a HIPAA compliant way. A business associate is any individual or entity that creates, receives, maintains, or stores PHI on behalf of a covered entity. Marketing agencies are considered a business associate to you, the covered entity. This can be done by entering into a BAA, to protect not only your patients, but you and your practice.

Marketing agencies may request exposure to PHI. PHI can be as small as a name paired with an email address or a cell phone number. A few examples include:

Your website

The most common example of PHI on a website is on a contact form that you want patients to submit. Most websites have a contact us page and every contact us page has a contact us form. The form always asks for a name, email, phone number, and then some information about the patient who is contacting the practice. That can be anything from “I'd like to make an appointment” all the way to describing detailed health history.

Email Correspondence

If you send regular emails or irregular emails, a name and email address is needed, and there may be an expectation of privacy in disclosing this information between the practice and the patient.

Patient Reviews

More and more healthcare practices are asking their patients to give them a review online. Many systems do so by sending emails or texts asking for reviews.

It's common for a marketing agency to manage some or all of these for their clients. Each of these may expose that agency to PHI, especially if information relating to the patient's condition, of even the physician specialty, is included in these requests, texts and emails.

What Makes a HIPAA Compliant Relationship with a Marketing Agency?

There are a few components to it.

1. The Marketing Agency Will Sign Your Business Associate Agreement (BAA)

A BAA is required by HIPAA, to protect patients and a provider. A BAA is a legal document that establishes the rules and requirements related to sharing PHI with a business associate. Good BAAs will include these four sections of coverage:

- **Who's Covered under the BAA** – including any employees of the Business Associate, and Covered Entity

- **What's Required of the Business Associate -** what's required with respect to protected health information and other areas of HIPAA that are relevant to the relationship you have with the marketing agency.

- **What's Required of the Covered Entity -** The second section is what's required of you, the covered entity, across those same areas.

- **What Happens if There's a Data Breach? -** What happens if there's a data breach? Who does what? What are the deadlines? How long do they have to report back? Who pays what costs?

You Need to Have Your Own BAA

As a covered entity you should have your own BAA that you use with third parties. A good healthcare attorney can draw one up for you. Every third party, from individuals to agencies, that could have access to PHI needs to sign your BAA.

2. The Agency Has Systems, Policies and Procedures in Place

Systems, policies and procedures are what keep safe the PHI you share with third parties. Systems, policies and procedures cover everything from how the agency encrypts data they send, how they store it (both physically and electronically), which employees are authorized to see it, and a number of other areas. You should find out if your marketing agency has systems, policies and procedures in place.

Do you really have to go through these steps? Won't the BAA handle this? No. A BAA is a legal document. It will reduce your legal risk, but it's not going to keep your data any safer than it was before. That's where systems, policies and procedures come in.

When you're looking for a marketing agency, you should ask them about their systems, policies and procedures. A good healthcare attorney and/or healthcare consultant that specializes in this space, can give you a good set of questions to ask to tease out what the agency has in place.

3. Do they Have HIPAA Compliant Relationships With Their Subcontractors?

The marketing agency should have BAAs in place with their own subcontractors. There needs to be an unbroken chain of BAAs for HIPAA compliance. The chain starts at the covered entity and goes all the way down to include whomever else that marketing agency subcontracts with to get their work done. Any breaks in the chain, could mean that PHI could be exposed to someone not authorized to see it.

4. Everything Else

Are there are other components that need to be in place? As we said at the start, we recommend you find a good healthcare attorney or healthcare consultant to guide you through all of the pieces to put in place to establish a HIPAA compliant relationship with any third party, including marketing agencies.

What If You're Working with an Agency That's Not HIPAA Compliant?

If you're already working with an agency, you're sharing PHI with them, but you don't have a HIPAA compliant relationship in place, we recommend that you correct that *immediately*. Find that healthcare attorney or SME in HIPAA healthcare consultant, get that BAA, and rely on what your healthcare HIPAA expert says and confirm their published guidance.

Start with your current agency. If they're not HIPAA compliant but will take the necessary steps, that's the easiest outcome for you. However, you might also find that they either can't comply or won't comply. It's not so easy to become HIPAA compliant and stay HIPAA compliant. But if you are in this situation, we really recommend that you switch agencies. It sounds painful, but you don't need the risk exposure of a non-compliant relationship.

To continue this conversation, or to get the expertise you need, to determine the right marketing agency for you and your practice, you can contact, Carl White at: whitec@marketvisorygroup.com or visit the NSCHBC.org website. Click on the "Find a Consultant" page, and type in your business needs, and our over 300+ members (Business Consultants) may be able to assist.