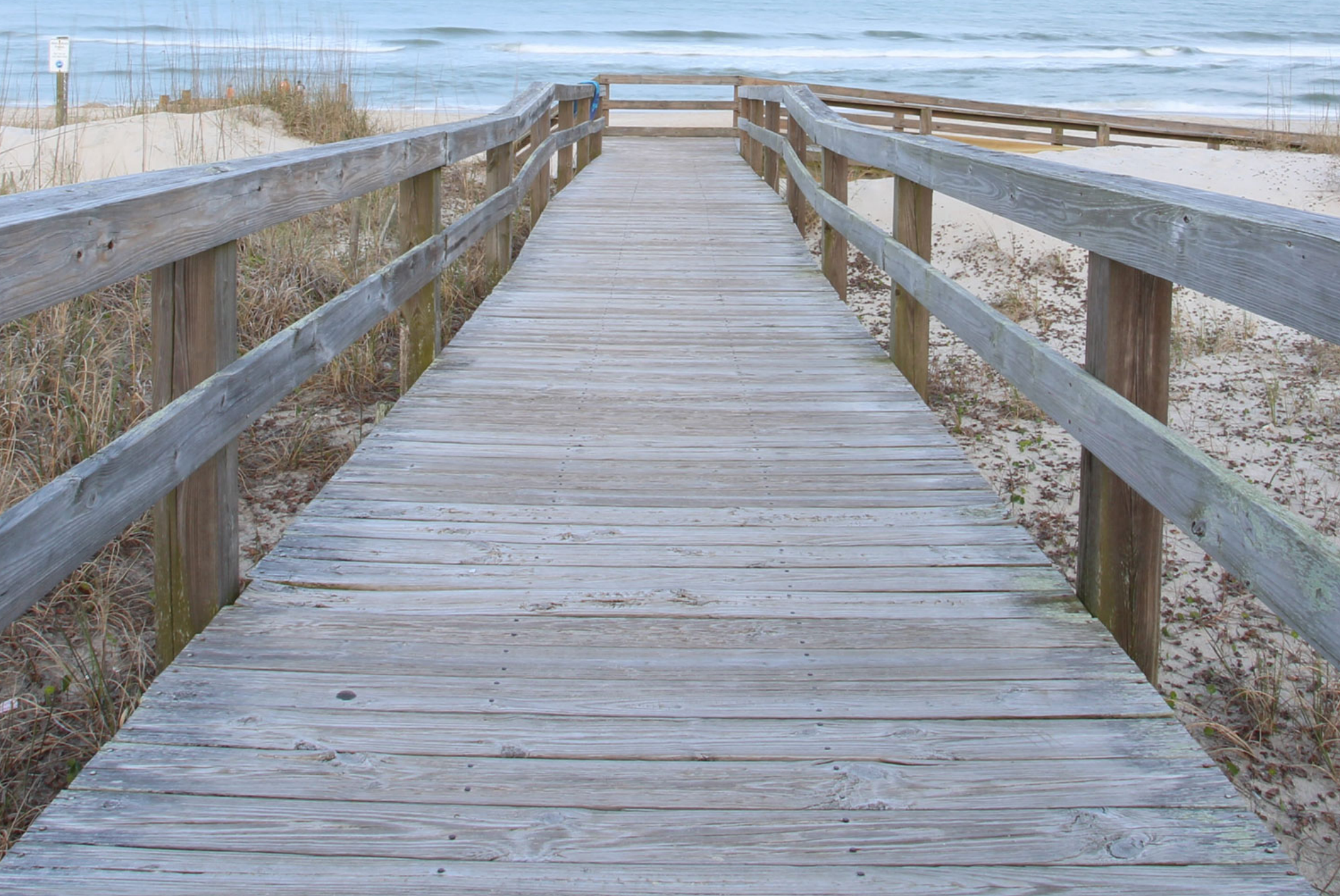
# HIPAA GUIDE

## A PRACTICAL GUIDE TO PROTECTING YOU AND YOUR CLIENTS

LEAN TOWARDS JOY, LLC



# HIPAA GUIDE

## A PRACTICAL GUIDE TO PROTECTING YOU AND YOUR CLIENTS

SECOND EDITION

LEAN TOWARDS JOY, LLC

# ARE YOU HIPAA COMPLIANT?

When I first set out to write this guide, I had a no idea about the complexity of the law. I understood its stated purpose was to protect the privacy of a client. Most people are aware of its obvious compliancy components. For example: don't share patient information, use encrypted communications, don't leave your laptop open and unlocked at a coffee shop while you get up for another refill, etc. These are all pretty obvious. However, they are just the tip of the iceberg.

HIPAA compliancy is a big deal. If you don't think it is worth the time to properly comply, consider the fines associated with a HIPAA violation. A simple "I didn't know" violation will cost you anywhere from $100 - $50,000 per violation. And if you don't think the U.S. Department of Health and Human Services is serious about enforcing its policies, just look at the case where they fined Alaska's own Department of Health and Human Services $1.7 million for an unencrypted USB hard drive being stolen. This fine was levied for poor policies and poor risk analysis. The Catholic Health Care Services of the Archdiocese of Philadelphia was fined $650,000 for one person's mobile device being stolen. The University of Massachusetts was fined $650,000 for a malware infection. And Lincare, Inc. (a medical supply provider) was fined $239,800 for unprotected documents affecting only 278 clients. How many current and past clients are in your records? Can you afford paying $862 per client for not following the proper guidelines?

I know I might have raised your heart rate a little with my introduction. It is not my intention to freak you out, only to get you to pay attention to the importance of being HIPAA compliant.

The Department of Health and Human Services Office of Civil Rights (OCR) is not a self-funded office. The agents working within the OCR receive their salaries from the federal government's budget. I mention this because it is important to know that the OCR does not have its eye on the citation. They are not looking to make money off the fines they levy. They are an organization that is truly passionate about protecting patients' information.

I have no doubt that you, too have a passion for your clients and the work you do with them. HIPAA violations are seldomly the result of malice actions. Most providers would not want any harm to come as a result of their client's protected information being disclosed. However, stuff happens. So, you want to make sure you take responsible actions to protect this information. Think of HIPAA as a nice guideline to follow. The writers of this law took into account all the ways information can get into the wrong hands and has laid out some rules to follow.

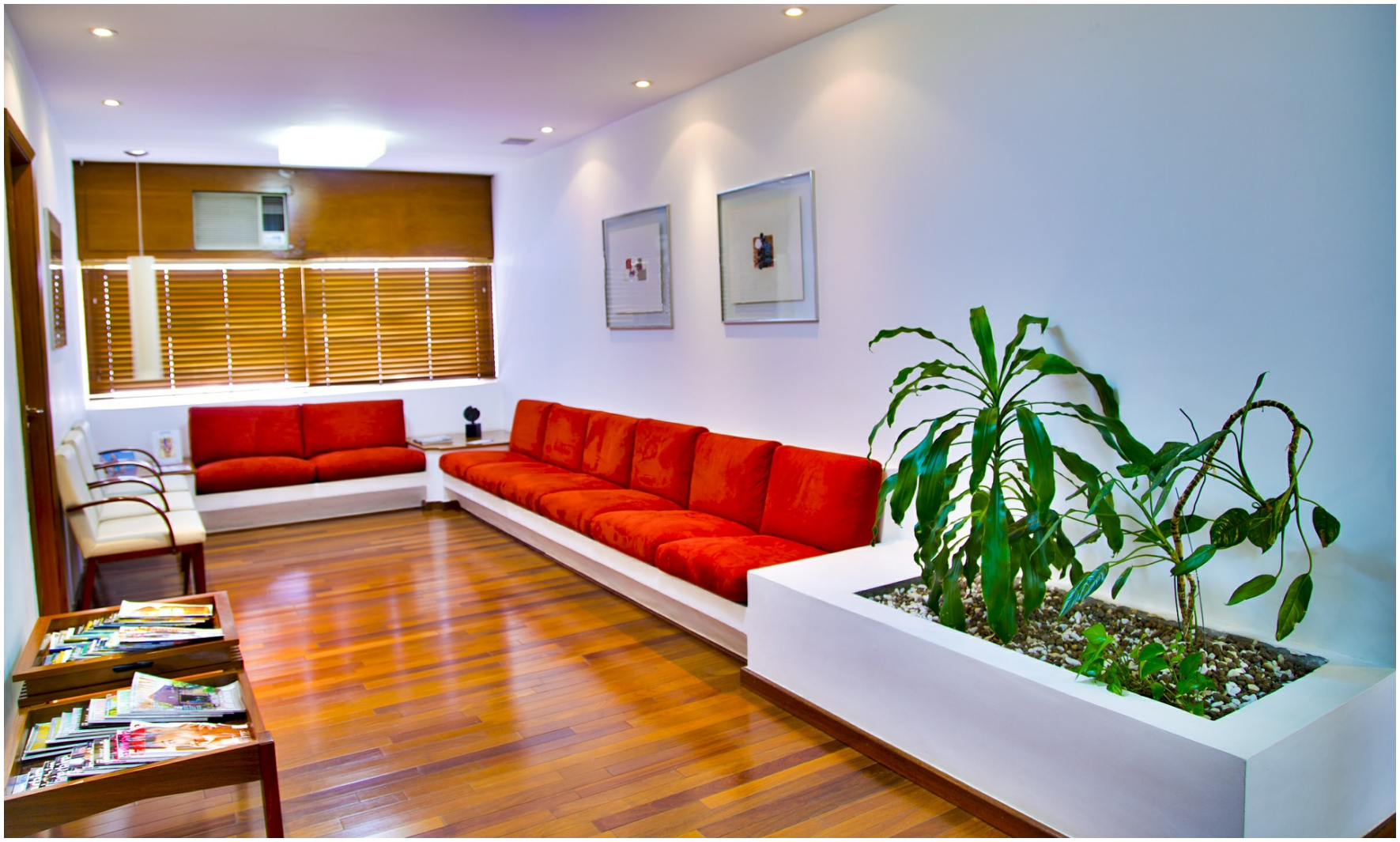
When you first set out on your heart-centered path for helping people, you did so with the moral intention of doing no harm to your clients. However, by not following proper HIPAA rules, you could potentially be putting your clients at risk. Unfortunately, for most practitioners, you won't realize the unauthorized use or disclosure of your clients' information until they have already been harmed.

So, who investigates HIPAA? The Office of Civil Rights (OCR)is tasked with enforcing the Privacy and Security Rules found within HIPAA (more on those later). However, more than likely you will not get a call from the OCR investigating your HIPAA compliancy unless they receive a breach notification by a business associate, an affected client, or an attorney for the opposing party. (*The latter example is usually seen with therapists involved in a custody dispute.*)

As you are reading this you might be counting all of your cohorts that are in violation of HIPAA; for some it can be comforting to know they are not alone. I see providers several times a week who are unknowingly violating HIPAA guidelines. The key is to start where you are. Now that you know you are doing something wrong or something that is not the "best practice", make a shift. Becoming HIPAA compliant will not only protect your clients, it will protect your organization.

The following information in this guide is meant to ease your transition into HIPAA compliancy. This guide is a broad overview of the key elements of HIPAA. This information is meant for educational and general information purposes. To make it easier for readers to comply with all the requirements of HIPAA and view the full text of the regulations, I have included links to the Office of Civil Rights (OCR) website at the end of this guide. The OCR office is within the Department of Health and Human Services.

# WHO IS THIS HIPAA GUIDE FOR?



## THIS GUIDE IS FOR EVERYONE

Whether you are a patient or a provider, it is important to know about HIPAA and what its practical applications are. HIPAA is not about compliance - it's about patient care.

## WHAT IF I ALREADY RECEIVED TRAINING FROM MY AGENCY?

More than likely if you are reading this guide you already know you need to be HIPAA compliant given your profession. Many licensed professionals are familiar with HIPAA through their training and from interning or working at an agency. However, usually the agency provided them with the training, policies, and procedures to stay HIPAA compliant within that agency. Once out on your own, you will need to develop new policies and procedures to stay compliant within your new environment.

## WHAT IF I DON'T NEED TO BE HIPAA COMPLIANT? WHY DO I NEED THIS?

HIPAA compliance is meant for more than just therapists and doctors. Covered entities are explored in more detail within the *Privacy Rule* section of this guide. However, regardless of the Department of Health and Human Services definition, I always advocate HIPAA compliance for any professional providing a healing service to a client. This includes, but is not limited to, Reiki practitioners, massage therapists, and acupuncturists.

Although a non-covered entity may not be held accountable by the Office of Civil Rights, it is still held accountable by its clients. Client care is the reason for your occupation and to protect their personal information is a continuation of that care. Clients assume a level of confidentiality when they use your services. Following the guidelines of HIPAA will protect your clients from unintentional disclosures of their information as well as protect you and your organization from civil lawsuits that could arise from such a disclosure.