Healthcare Insurance Portability and Accountability Act (HIPAA) Compliance or Best Business Practices for the Holistic Nutrition Professional

---

NANP
National Association of Nutrition Professionals

LEGISLATIVE AFFAIRS DIVISION

nanp.org

This document aims to clarify the regulations of the Healthcare Insurance Portability and Accountability Act (HIPAA) and how these regulations impact Holistic Nutrition Professionals. It will also provide information on best business practices for Holistic Nutrition Professionals who are not required to comply with HIPAA regulations.

The Health Insurance Portability and Accountability Act (HIPAA) program is under the purview of the Health and Human Services Department and was enacted as a law in 1996 to protect a patient's right to confidentiality, combat fraud, and develop industry-wide standards for records management and electronic filing. The law defines who must be compliant, and these providers are referred to as "covered entities." HIPAA covered entities include health plans, clearinghouses, and certain health care providers as follows:

For HIPAA purposes, health plans include:

- health insurance companies
- HMOs, or Health Maintenance Organizations
- employer-sponsored health plans
- government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs such as TRICARE

Clearinghouses include organizations that process health information such as medical billing companies that function as intermediaries from healthcare providers to insurance payers.

Providers who submit electronic claims are also considered covered entities. These providers include, but are not limited to:

- doctors
- clinics
- psychologists
- psychiatrists
- dentists
- chiropractors
- nursing homes
- pharmacies

How do I know if I need to comply with HIPAA regulations?

The majority of Holistic Nutrition Professionals do not work as "covered entities" and therefore are not required to be HIPAA compliant. Those practitioners who work for covered entities such as pharmacies, or licensed medical professionals are covered under that provider's license. In these cases, the Holistic Nutrition Professional may be considered a "business associate." This is defined as a person who does not create, receive, maintain or transmit Protected Health Information (PHI) in their primary occupation, but who provides third party services and activities for covered entities during which they will encounter PHI. Before undertaking a service or activity on behalf of a covered entity, a business associate must sign a Business Associate Agreement guaranteeing to ensure the integrity of any PHI to which it has access.

How do I determine if I need to be HIPAA compliant?

The best way to determine if you must comply with HIPAA regulations is to ask yourself the questions below. Practitioners who answer "No" to these questions are not considered a covered entity or business associate and are not required to adhere to HIPAA regulations.

(1) Do I receive payment for providing healthcare services?

Most Holistic Nutrition Professionals do not. HIPAA defines "healthcare services" as services provided by a licensed medical professional whose scope of practice includes diagnosing, treating, prescribing, healing, or curing diseases. This falls outside the scope of practice of Holistic Nutrition Professionals unless they are also licensed medical professionals.

(2) Do I transmit personal health information electronically to a third party?

If you transmit information to insurance companies or licensed healthcare professionals then you should be HIPAA compliant. Information that you send directly to your client is not considered a third-party transmission and therefore does not require HIPAA compliance.

What business best practices should I follow if I am not required to be HIPAA compliant?

Holistic Nutrition Professionals should always follow best practices to protect their clients' personal information. You as a practitioner should make every reasonable effort to prevent anyone from accessing your clients' personal information. This includes names, addresses, credit card numbers, email addresses, photos of your clients, and medical records provided to you by your client or a licensed medical professional. You should also clearly state in your waiver/disclaimer documents your intention to protect your clients' personal information.

The following are best practice guidelines to protect you and your clients:

- Password protect your computer where client files are stored.
- Paper files should be locked in a file cabinet, especially if you share office space.
- Do not discuss clients with other people or practitioners without express written permission from your client.
- Have your clients sign your waiver/disclaimer emphasizing that you are not licensed or certified by the state and that you are not able to diagnose, prevent, treat, prescribe, heal or cure any disease. Also, make sure that you state your intention to protect their personal information.
- Always recommend that your clients seek medical advice from a licensed health care practitioner.
- For those practitioners who reside in states where they can legally provide telehealth services, you must be aware of specific requirements for computer software. Examples of HIPAA compliant software include Zoom Health, Practice Better, Doxy.me, VSee, TheraPlatform, Simple Practice, TheraNest, TheraLink, and PracticeSuite. You can find further information about computer security here: https://www.hhs.gov/hipaa/for-professionals/security/index.html

How long should I retain client information/files?

This varies by state, however, a good rule of thumb is to retain client files for at least six (6) years. When that time has passed, you may shred any hardcopy documents or erase computer files. It's best to contact your client before purging this information and offer to provide them with their files.