



PATIENT RIGHTS

PATIENT RIGHTS



The material in this section is a combination of rights from that are listed under the Federal, NC Resident Rights, Raise The Bar Therapy Services handbook and administrative. The material that was selected was pertinent to rehab services and is not a complete list of Patient Rights.

Patient Abuse and Neglect

- All patients of Raise The Bar Therapy Services (RTBTS) llc., have the right to be treated and provided services with dignity and respect, free from any abusive treatment, neglect or exploitation, including the use of abusive language.
- RTBTS has zero tolerance for any type of patient abuse, neglect, exploitation, or mistreatment. Any employee found to have committed or conspired with another or fails to report an act of neglect, abuse, or exploitation will be terminated and reported to the state regulatory agency. If appropriate, licensing officials, and or law enforcement will be contacted.
- In addition, an employee who fails to report a confirmed or suspected abuse of a patient by any other person (including family member, other staff, or another patient) will be reprimanded and held accountable.
- The patient has the right to voice grievances regarding treatment and care without the fear of reprisal, restraint, interference, coercion or discrimination and to have prompt efforts undertaken by the administrator to resolve them.

PARTICIPATION IN THE PLAN OF CARE

- As stated in the RTBTS P & P Manual, the patient has the right to be involved in the development of the plan of care, display an understanding of treatment modalities, and discharge planning as applicable.
- The patient has the right to receive care, treatment, and services that are adequate and appropriate and in compliance with the relevant state and federal rules.
- If there is a language or cognitive barrier, the patient will be provided with an interpreter and/or family support will be provided to assist the patient in gaining a complete understanding, where possible, of the plan of care.
- The patient has the right to refuse treatment.

HIPAA AND PHI COMPLIANCE

What is HIPAA?

Passed by Congress in 1996, HIPAA is a dense piece of legislation that has serious implications for virtually all medical professionals, including physical therapists, occupational therapists, and speech-language pathologists. All HIPAA-covered entities (e.g., healthcare providers, insurers, and business associates) must follow certain rules governing the way PHI is collected, shared, and used.

While you may think that HIPAA violations are significantly more likely to happen to large insurance carriers or major healthcare organizations, the [US Department of Health & Human Services](#) (HHS) says that private practices are the most common type of covered entities “that have been required to take corrective action to achieve voluntary compliance,” coming in ahead of hospitals, outpatient facilities, pharmacies, and health plans.

What's PHI?

PHI includes:

- patient demographic information
- medical history
- test and laboratory results
- insurance information
- other data used to identify individual patients and develop plans of care

What are the consequences of non-compliance?

HIPAA violations include anything from talking about identifiable patient information with your friends and family members to using FaceTime to discuss PHI in a public place. Such violations could have very serious implications for rehab therapists and their clinics. Those found to have wrongfully disclosed individually identifiable health information are subject to both financial and criminal repercussions—[including fines of up to \\$50,000 and a year of imprisonment.](#)

According to the [HHS](#), since April 2003—when compliance with [HIPAA](#) standards became mandatory—the Office for Civil Rights (OCR) “has received over 197,049 HIPAA complaints and has initiated over 924 compliance reviews.” Of those reviews, here are the top four most-investigated compliance issues:

1. Impermissible uses and disclosures of PHI
2. Lack of safeguards of hard copy and electronic PHI
3. Inability for patients to access their PHI
4. Use or disclosure of more than the minimum necessary PHI

What should I do if I suspect a HIPAA breach?

Research

Healthcare providers are legally obligated to research any suspected breach, no matter what. This means that your practice must immediately determine the size and scope of the incident to assess whether the probability that PHI has been compromised is high or low. Medical Economics recommends performing a risk assessment based on the answers to the following questions:

- What is the nature and extent of the PHI involved? What types of identifiers does the data include, and how easily could they be re-identified?
 - Who received or used the PHI?
 - Was the PHI acquired or viewed?
 - Has the risk to the PHI been mitigated? If so, to what extent?
- Additionally, you should identify the number of affected patient records, because this number will determine how you handle the next step.

Disclose

The way you handle post-breach disclosure communication is incredibly important. As much as you may wish you could keep the breach quiet, well-timed and strategic communications with your patients, employees, business partners, and vendors will help manage patient concerns and minimize the spread of misinformation. Plus, your practice is legally required to notify the affected patients—regardless of the scope of the breach.

However, there are two additional reporting requirements that do depend on the size of the incident:

Fewer than 500 Individuals

According to [HHS](#), if the breach affects fewer than 500 patients, your clinic isn't under much of a time crunch. So long as you report the breach to the Office for Civil Rights (OCR) "within 60 days of the end of the calendar year in which the breach was discovered," you've fulfilled your reporting requirements (though you can report sooner, if you'd like).

500 or More Individuals

However, if the breach affects 500 or more patients, your clinic must report the breach electronically "without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach." [This Healthcare IT News article](#) explains that if you do need to report the breach to the OCR, you'll need to document several key pieces of information, including:

- the number of impacted patients
- your practice's efforts to notify those patients

- a description of the type of PHI that was compromised
- steps individual patients should take to protect their privacy
- a description of your damage-control efforts and how you plan to prevent future breaches

Your practice also must report the breach to the news media. And it's important to note that if a breach is large, your practice likely will attract a lot of media attention. So, make sure your employees know not to engage with members of the press without approval or appropriate messaging. Better yet, consider [retaining an experienced public relations firm](#).

For more guidance on who to notify and when, read [this page](#).

Crunch the Numbers

Brace yourself, because there will be financial fallout. Even if your practice has a reserve of funds earmarked for emergencies such as this, you may still be in for a shock. Between the costs of investigating the breach, obtaining PR services, and making necessary IT security upgrades—not to mention the potential lawsuits and OCR fines—your practice stands to lose and/or spend a lot of money in a short amount of time. Moreover, losing patient trust could really hurt your bottom line. That's why it's imperative that you communicate smartly and quickly—and create a plan to prevent another breach from occurring in the future.

What's the HIPAA Omnibus Rule?

In 2013, the Department of Health and Human Services (HHS) beefed up HIPAA's regulations and violation penalties with the [HIPAA Omnibus Rule](#). Among other things, this rule expands the liability of business associates, further restricts the use of PHI for marketing purposes, and strengthens patients' rights to obtain copies of their health information. According to [this executive summary](#), the changes:

- Hold business associates and covered entities liable for some aspects of HIPAA compliance.
- Prevent the unauthorized sale of PHI and restrict the use and disclosure of PHI for marketing and fundraising.

- Provide individuals with the authority to obtain electronic copies of their health records and decline to disclose information related to a treatment paid for out-of-pocket.
- Mandate that covered entities update and redistribute their notices of privacy practices (NPPs).
- Change certain requirements related to the disclosure of health information with the intent to facilitate research and the disclosure of childhood immunization records.
- Allow family members to access the health records of their decedents.
- Enforce penalties for noncompliance that arise from willful neglect and establish an objective standard for the “harm” threshold.
- Prohibit health plans from using or disclosing genetic information for underwriting.
- Amend the civil monetary penalties. (See table below.)

The table below, modified from the [Federal Register](#), displays the range of penalty amounts for civil breaches. We’re not even going to address criminal ones, because we know you would never intentionally do such a thing.

Table 2—Categories of Violations and Respective Penalty Amounts

Violation category— Section 1176(a)(1)	Each Violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	\$100– \$50,000	\$1,500,000
(B) Reasonable Cause	\$1,000– \$50,000	\$1,500,000
(C)(i) Willful Neglect- Corrected	\$10,000– \$50,000	\$1,500,000
(C)(ii) Willful Neglect-Not Corrected	\$50,000	\$1,500,000

How can I keep my clinic HIPAA-compliant?

Digital Security

Get the Right EMR

Obviously, the government doesn't take PHI protection lightly. But don't worry; there are lots of ways to ensure that you and your clinic have the resources and internal processes crucial to achieving full HIPAA compliance. Step one is making sure your patient records are stored securely—[within a HIPAA-compliant EMR](#), for example.

WebPT provides unique user IDs and passwords for each therapist, PTA, front-office staff member, and administrator. That way, clinic owners can control access to PHI. And with secure data centers, featuring defensible perimeter, digital video surveillance, biometric screening, and round-the-clock guard staff, your data receives top-level security. Still have concerns about storing your patients' information electronically? Consider this: In 2018, WebPT obtained its [International Standardization Organization \(ISO\) certification](#), making it the first ISO-certified EMR designed specifically for rehab therapists. What does that mean? Being ISO-certified means WebPT securely manages all its sensitive data—including financial information, patient details, Member data, and medical record data hosted by WebPT's third-party vendors and partners. Plus, WebPT's ISO certification—along with its existing compliance safeguards—further demonstrates the company's commitment to data security for all Members.

Learn more about our [gold-standard security here](#).

Create Safe and Secure Passwords

Chances are good that you're using more than one web app as part of your clinic's daily operations—and each application requires a password that is challenging enough to be safe, but a password recovery process that doesn't bring operations to a halt if you or someone on your staff forgets which password opens which application. Because HIPAA has some strict guidelines around password security, we recommend using a password management system to oversee all your letter, number, and special character combinations.

Here are three:

1. [LastPass](#) works on your phone, tablet, or desktop computer and integrates with most browsers. To put it simply, LastPass helps ensure that your web passwords are both strong and secure. It also works exceptionally well on Macs (unlike some of the other options) and there's a premium service that alerts you about relevant security issues.
2. [KeePass](#) stores passwords and data in local files on your computer. This makes sharing data a bit more challenging, but you can use it with DropBox, Google Drive, or other file-sharing programs. KeePass also is super portable (you can load it onto a thumb drive); works well with Mac, Windows, and Linux; and is totally free. It offers a hands-on sort of password management, but it's still a good option if you're willing to deal with plugins and files.
3. [1Password](#) is a well-designed and easy-to-use product. In addition to being pretty, 1Password has some unique features that make it a techie favorite. First, it's easy to set up on your PC, either with local files or via a syncing system that runs through the cloud. It also offers a digital wallet for storing credit cards and addresses for easy checkout when making online purchases.

If none of these spark your interest, there are plenty more, but they all have a few commonalities: they're all centrally managed with a single-password entry system—and they allow users to step up security with two-factor authentication. As a result, you'll be able to maintain strong, secure passwords while ensuring everyone who needs access has it.

Encrypt and Back Up Your Data

Encryption has been around since, well, cavemen and cavewomen etched encoded images into cave walls. But in today's small-business world, it's an often-overlooked solution to preventing unauthorized access to high-risk data. If you're a WebPT Member, you can rest a little easier knowing that the WebPT application is well encrypted at every level. However, you should still consider encrypting your workstation with either BitLocker (Windows) or FileVault (Mac).

Both products encrypt your entire hard drive and secure your data. Just make sure that when you implement one of them, you store the keys

created during the encryption process in a safe (read: locked) space. While we're on the topic of safe spaces, consider this: all portable storage should be encrypted as well. That way, if any flash drives or external hard drives are lost or stolen, your data remains protected. Speaking of portable data storage, mobile devices such as smartphones and tablets are another cause for security concern. Several HIPAA investigations have resulted in providers receiving fines because their unencrypted mobile devices contained electronic PHI (ePHI) or stored passwords that non-authorized individuals could use to access cloud-stored data. In this day and age, you must set lock-screen combinations and encrypt your devices. It's just too easy to misplace or lose tablets and phones during work or travel.

If you're a WebPT Member, you're covered when it comes to backing up the files that contain your critical EMR data. That's right—we store it all and keep it safe. But we can't do much of anything to protect all of the other data your clinic uses, so please be sure to implement a solid backup process to cover everything else.

Install Antivirus and Malware Protection

A lot of questions arise during discussions about antivirus and malware, probably because there are a lot of options from which to choose. While many of them are good, you need one that's great. In other words, you need one that provides regular and intensive updates and immediate fixes to address the nastiest of Internet viruses.

WebPT recently completed an exhaustive search to identify our next antivirus solution, and we found three great options: Sophos, BitDefender, and ESET. Here's why they made our cut:

- They work well for both Apple and Windows machines.
- They perform active and passive scanning of workstations and any removable storage devices plugged into those workstations.
- They're centrally managed via on-premise devices or the cloud.
- They're easy to install.
- They provide consistent updates.

We recommend all three without hesitation, but whichever solution you chose, be sure to install it on all of your devices, including your phones and tablets.

Social Media

Your patients are [using social media](#) to make informed decisions about their health, so as a smart healthcare provider, you should be using social media, too. But because of non-compliance concerns, you also must be prudent with its use. After all, social media is anything but private—and it's practically permanent, because once you put something online, chances are good it's going to live forever. You might think you deleted that unfortunate tweet or photo, but if someone took a screenshot of it, it's most definitely not gone for good.

That's why your clinic should develop—and enforce—a [social media policy](#) that takes HIPAA compliance into consideration. Here are seven tips for keeping your practice socially safe:

1. Supervise staff members who handle your social media platforms.
2. Train your staff on social media and [your social media policy](#).
3. Establish a system to track, archive, and retrieve electronic communications, just in case you need them as evidence should you ever find yourself facing a lawsuit.
4. Approve content before it gets posted. If this isn't possible, [Forbes suggests](#) implementing technology that monitors real-time social media posts for you—and flags posts with non-compliance potential.
5. Create pre-approved content and short snippets of text your staff can use to provide regular—and consistent—status updates. These also come in handy whenever staff need to quickly respond to patients in sticky situations.
6. [Do not give out medical advice](#) or include PHI on social media—ever.
7. Monitor your social media accounts regularly to ensure your staff is using them appropriately. If you find cause for concern, be sure to enforce your policy—including the consequences.

Email

Just like all other facets of your business, your email marketing must adhere to HIPAA rules.

Unfortunately, the HIPAA rules around marketing are pretty murky—especially since the introduction of the 2013 HIPAA omnibus ruling. So, to cover your bases, include a marketing communications opt-in form as part of your intake packet. That way, there's no question as to whether you can market to your patients via email. Within your opt-in form, clearly explain the types of communications they'll receive from you. If a patient is hesitant to opt in, explain how those communications will benefit him or her. And if the patient still chooses not to opt in, respect that decision and don't try to pressure him or her into it.

Legally, you must provide a clear avenue for your opt-ins to unsubscribe at any time. And if a subscriber asks you to unsubscribe him or her, you absolutely must comply.

Speaking of legalities, remember that the email addresses you collect are considered PHI. Thus, you must handle them accordingly. On that note, be sure to verify that your email software vendor understands HIPAA and that it'll work with you to ensure compliance.

Wearable Technology

Lots of people are sporting activity trackers like Fitbit, Jawbone's Up, Nike's FuelBand, and Apple's iWatch, which means individuals, businesses, and healthcare professionals can easily monitor physical activity of all kinds. And where there's fitness activity data, there's also PHI. That means these seemingly insecure devices are chock full of protected health information, which is leading many experts to question whether wearable technology is HIPAA-compliant. In most cases, the answer is "no."

The Gray Area

HIPAA doesn't directly mention wearables—at least not yet—which leaves [a legal gray area](#) between health data collected for personal use and health data collected by or for a HIPAA-covered entity. Most wearables manufacturers are not at all capable of being able to analyze, share, and secure health data in compliance with HIPAA regulations.

Data for Sale

According to [SearchHealthIT](#): “Non-covered entities can often do whatever they want with someone’s data as long as those potential actions are included in the terms and conditions—which are rarely ever read by users—including sharing and selling data.”

And speaking of selling data, a [recent review](#) in Science Translational Medicine provides some anxiety-producing statistics for wearables consumers: “The U.S. Federal Trade Commission recently tested 12mHealth and fitness apps and found that consumer data from these apps were being sent to 76 different third-party companies. Some of the data shared include the phone’s unique device identifier as well as the owner’s running routes, dietary habits, and sleep patterns. A similar analysis of 43 fitness apps found that 40% were collecting what was classified as high-risk data—addresses, financial information, full name, health information, location, date of birth, or zip code—and more than 55% were sharing data with third-party analytical services that could potentially link those data with data from other apps.”