TECHNOLOGY FOR PSYCH PROFESSIONALS:

Protecting Data to Minimize Malpractice and Other Liability Claims

insureon

insureon

TABLE OF CONTENTS

INTRODUCTION

Mental health professionals of all types – psychologists, social workers, counselors, and therapists – may not think technology is one of their industry's growing concerns. After all, in this field, you deal with life-altering crises such as trauma, divorce, depression, anxiety, and behavioral issues all the time. Keeping up with the latest tech liability issues is probably low on your to-do list.

But part of helping your patients involves protecting their highly sensitive health information. HIPAA laws govern how mental health professionals must store data and communicate with patients or clients. In a digital workplace, those seemingly cut-and-dry regulations can get blurry fast. Still, you must understand and comply with these regulations if you want to avoid data breaches and regulatory fines.

That's where this guide can help. In this eBook, we'll explore...

- The reality of how Americans use electronic communications for healthcare purposes.
- How HIPAA's privacy and security standards work.
- Examples of HIPAA violations that quickly lead to lawsuits.
- Social media risks mental health professionals may encounter.
- How to use technology without running afoul of HIPAA and inviting breaches, lawsuits, and fines.

Read on to learn more.

CHAPTER 1

HEALTH INFORMATION ONLINE:
WHAT YOUR PATIENTS ARE DOING, WHAT PROFESSIONALS ARE DOING

HEALTH INFORMATION ONLINE: WHAT YOUR PATIENTS ARE DOING, WHAT PROFESSIONALS ARE DOING

Perhaps the first step toward identifying the risks your mental health practice may experience in a digital world is to understand how your clients and fellow professionals use the Internet to manage healthcare issues. Though we could discuss the merits and drawbacks of using the Internet to access and explore health information, we won't. At the end of the day, all that matters is that people rely on digital health records and expect them to be available online.

For example, according to a study by Pew Research Center's Internet & American Life Project...

- **72 percent** of Internet users went online for some kind of health information in the last year.
- **35 percent** of American adults have gone online to figure out a medical condition.
- **46 percent** of those surveyed said their online findings prompted them to seek medical care.
- **41 percent** of "self diagnosers" found medical professionals confirmed their diagnosis, while 35 percent didn't get a professional opinion.
- **11 percent** of those who post online about medical concerns are specifically looking for feedback from a medical professional.

72% of Internet users went online for some kind of health information in the last year.

That doesn't mean it's only your clients and patients who are taking to the Internet to manage their health and make their lives easier. Allied health practitioners use the Internet just as much, but for different reasons:

- Some use the Internet to answer questions online diagnosers have.
- Some simply find it to be an easier way to reach their patients.
- Others use blogs and social media to promote their practice, connect with other allied health professionals, and educate others about their work.

But these kinds of use can lead to malpractice suits, privacy violations, and other problems. The Federation of State Medical Boards (FSMB) reports that when US Executive Directors at state medical boards were surveyed in 2010, **92 percent** found violations of online professionalism reported in their jurisdiction.

Specifically...

- **69 percent** of violations were over using the Internet to inappropriately contact patients.
- **63 percent** involved using the Internet to inappropriately prescribe.
- **60 percent** of violations involved misrepresenting credentials or clinical outcomes online.

For these violations, **71 percent** of boards held formal disciplinary proceedings to limit, suspend, or revoke licensure. **Forty percent** issued informal warnings.

92% of state medical boards reported online violations of professional standards.

That's why it's essential to know how to appropriately interact with patients and clients online. You've worked too hard to build your mental health practice to leave its reputation unguarded. So when you want to connect with others online and offer advice about mental health issues, follow the FMSB's advice. It recommends that you...

- **Disclose information** and explanations of how to use it for any healthcare services offered online.
- **Protect patient privacy and data**, ensuring that "de-identified" data can't be connected to a patient (granted, this is harder than you might think. More on that in Chapter 3).
- **Ensure all information is truthful,** current, accessible, and straightforward.

This brings us to our final point: conversations about mental health are happening online every day. Though participating in these conversations does come with risks, it also offers you the chance to build up your practice's credibility and help you connect with patients. Plus, these days, patients expect to be able to discuss their conditions with others online and to communicate electronically with practitioners via email or social media.

That means you have your work cut out for you as far as balancing professionalism, privacy laws, and client expectations. Let's take an in-depth look at how you can keep your mental health practice compliant while navigating the digital world.

CHAPTER 2

HIPAA FOR MENTAL HEALTH PRACTITIONERS

HIPAA FOR MENTAL HEALTH PRACTITIONERS

Chances are, you didn't make it this far in your field without knowing what HIPAA is and what it regulates. But for the sake of covering bases, let's briefly recap the HIPAA takeaways that relate to cyber privacy issues.

First Things First: Who's Covered by HIPAA?

You're covered by HIPAA (and must comply) if...

- **You are a covered entity.** This includes any business that electronically bills or checks health insurance coverage eligibility using a computer or web-based system.
- **You engage in covered transactions.** This includes computer-to-computer transmission of healthcare claims, payment and remittance, benefit information, health plan eligibility information, any digital bills submitted to insurers, and any digital billing information submitted to clients.

As you may already know, Title II of HIPAA is the part of the law that most applies to your electronic work. It governs the privacy, security, and electronic transfer of healthcare information.

According to the Clinical Social Work Association, there's another key part of HIPAA that is especially important for mental health practitioners. HIPAA adopted the *Current Procedural Terminology* (CPT) for procedure codes and *International Classification of Diseases* (ICD) for diagnoses. The latest version of the DSM uses the diagnostic codes in the ICD, which should make everyone's life easier.

Your practice is covered by HIPAA if you check health insurance coverage using a computer, transmit healthcare claims, or submit digital billing information to clients.

HIPAA Privacy Standards vs. Security Standards

HIPAA also set up privacy and security standards, which can be easy to confuse. For clarity's sake, here's the difference:

- **Privacy standards** establish who has the right to disclose and use protected health information (PHI) and under what circumstances, whether the information is expressed orally, in writing, or through electronic transmission. The standards also mandate that "reasonable steps" must be taken to secure PHI according to the HIPAA Privacy Rule.
- **Security standards** offer guidance on what administrative, physical, and technical measures should be taken to protect electronically stored or transmitted PHI from corruption by viruses, theft by cybercriminals, and transmission on unsecured channels.

Both the HIPAA Privacy and Security Rules seek to protect and secure electronic "individually identifiable health information," which includes...

- The individual's past, present, or future physical or mental health or condition.
- Healthcare procedures and services provided to the individual.
- The past, present, or future payment for the healthcare the individual received (including diagnoses, treatments, prescriptions, etc.).
- The patient's name, address, birth date, Social Security Number, and other identifiers.

Privacy standards dictate how information can be used and security standards dictate how information must be protected.

So How Should You Protect e-PHI, Anyway?

When it comes to protecting e-PHI, "reasonable steps" doesn't offer much guidance. And that's where HIPAA's security standards can help. They provide the following guidelines on how to keep your patients' healthcare information safe from prying eyes:

- **Analyze the risks.** You have to know where the vulnerabilities are before you can create effective safety protocols. It's best to document the potential risks for e-PHI exploitation and any security measures you adopt to address those risks. Be sure to update your risk management approach when necessary.
- **Put administrative safeguards in place.** This means designating a security official who is responsible for developing and overseeing security procedures, limiting disclosures of PHI, and training your employees on the proper management of e-PHI.
- **Put physical safeguards in place.** Limit physical access to the facilities where e-PHI is stored and only allow authorized access to these areas. Be sure to create and follow procedures that outline the proper use of workstations and electronic media. Your policies should also detail how to safely transfer, remove, and dispose of e-PHI or the devices that store it.

- **Put technical safeguards in place.** Only allow authorized personnel to access e-PHI. Use hardware, software, and procedural mechanisms to keep track of who accesses e-PHI on your systems. Lastly, implement network security measures that block unauthorized access to e-PHI that is being transmitted over your network.

For a more exhaustive and detailed exploration of the guidelines, check out the HHS's Summary of the HIPAA Security Rule and Privacy Rule.

Why HIPAA Matters for Mental Health Practitioners

Though there's a lot to keep track of in HIPAA's regulations, it's the law of the land. Failure to comply could result in...

- Losing your credentials or licensure.
- Fines.
- Lawsuits.

If that last bullet point comes as a surprise, maybe it's time to brush up on the 2014 HIPAA-related court case in Connecticut. This case opened the door to lawsuits against healthcare providers over HIPAA violations.

How HIPAA Violations Can Be Considered a Form of Negligence

In 2014, a court case opened the door to suing healthcare providers over HIPAA violations. This is a big deal because, prior to the lawsuit, it was unclear whether adhering to HIPAA could be considered a professional duty and whether failing to uphold HIPAA could be considered a professional liability violation.

HIPAA noncompliance can result in revoked licensure, fines, and lawsuits.

Here's what happened, according to HealthITSecurity:

- A patient of Westport, Connecticut-based Avery Center for Obstetrics and Gynecology instructed the Center not to disclose her medical information to the father of her child.
- Avery received a court subpoena to disclose the patient's health information.
- Avery complied with the court, handing over the record. It did not notify the patient or ask for legal guidance before doing so.
- The patient sued Avery for negligence, claiming that it had a duty to maintain her confidentiality.
- The Connecticut Supreme Court ruled in favor of the patient, effectively introducing the possibility of negligence suits against healthcare practitioners who violate HIPAA.

Before this ruling, individuals could not file such a lawsuit. The closest they could get to suing over HIPAA violations would be to file an invasion of privacy suit. But this latest ruling views HIPAA violations as a form of negligence.

This development is especially troubling for mental health practitioners like social workers who are often subpoenaed to disclose confidential information about their charges.

And that's not all. According to The Healthcare Blog, Walgreens was successfully sued over a HIPAA violation in 2013 – to the tune of **$1.44 million**, no less. A Walgreens pharmacist looked up her husband's ex-girlfriend's medical file under the suspicion that the ex had passed along an STD to him. Once she uncovered the information, she told her husband, who then texted the ex-girlfriend. Naturally, the ex sued Walgreens, claiming it failed to properly supervise and educate its employee about HIPAA regulations.

A Connecticut judge ruled that HIPAA violations can be a form of negligence, which greenlights malpractice suits over confidentiality breaches.

In this case, the judge determined that under Missouri law, HIPAA could be used to establish a legal duty of care, which informed the ruling against Walgreens. Such a lawsuit could also establish precedence for future lawsuits over HIPAA violations that happen via text, social media, and other kinds of electronic communications.

For both cases, Malpractice Insurance (also called Professional Liability or Errors & Omissions) could cover the cost of defending your practice against these claims because both judges determined that HIPAA is a standard of care and violations of it are a form of negligence. Professional Liability Insurance can cover the legal costs associated with professional negligence claims, but we'll go over that in more detail in the next chapter.

This brings us to the next hot topic: how social media and HIPAA intersect and collide for social workers, psychologists, and therapists.

CHAPTER 3

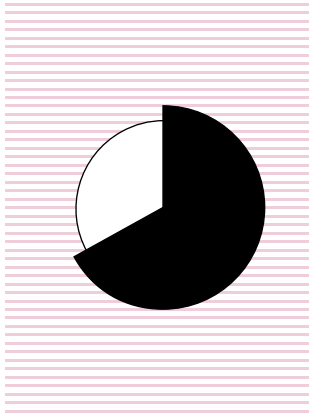
AN INTRODUCTION TO SOCIAL MEDIA STANDARDS FOR MENTAL HEALTH PROFESSIONALS

AN INTRODUCTION TO SOCIAL MEDIA STANDARDS FOR MENTAL HEALTH PROFESSIONALS

In general, mental health professionals have to consider two sets of rules when implementing technology in their practices:

1. HIPAA rules for maintaining privacy and data security.
2. Codes of ethics outlined by their respective professional organizations.

That means the stakes are high when it comes to using social media. Remember that practitioners may be sued over HIPAA violations, and if they break their industry's code of ethics, they could lose their licensure or face other penalties. And while the Federation of State Medical Boards (FSMB) Special Committee on Ethics and Professionalism developed guidelines for state medical boards to consider when teaching licensees about appropriate conduct while interacting via social media, email, text, and other forms of electronic communication, those guidelines aren't hard-and-fast rules that you can follow to the letter.



67% of allied health practitioners use social media professionally.

Instead, you have to know your risks and use your professional judgment and pay attention to the advice of the organizations built to oversee this kind of ethical gray area.

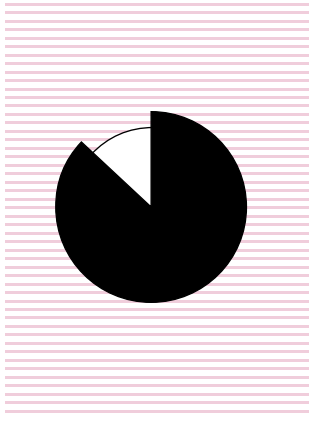
For example, the FSMB discourages medical practitioners from interacting with patients and clients on social media. Still, according to a survey by QuantiaMD, **67 percent** of practitioners use social media for professional purposes. Plus, other research compiled by the FSMB found that...

- **35 percent** of medical practitioners have gotten friend requests from patients or family members.
- **16 percent** of practitioners have visited an online profile of a patient or family member.
- **17 percent** of practitioners included enough identifying information about patients on social media that they could be identified.

From these numbers, you can see that social media use often blurs the boundaries of professionalism, and if practitioners share their work experiences online, there's the potential to violate patient privacy and confidentiality. As we explored in the last chapter, these HIPAA violations can be construed as negligence and lead to lawsuits.

Then there's the issue of grouping your personal and professional social media accounts together. If you're like **87 percent** of the medical practitioners surveyed by QuantiaMD, you probably use social media for personal purposes. If you run your own practice, combining your personal and professional accounts may seem like a good way to streamline your online activity. But it's always safer to keep personal and professional accounts cleanly separated.

There's a lot of nuance here, so we're going to break these issues down based on profession. Let's take a look at social media risks and best practices for social workers, psychologists, therapists, and counselors based on HIPAA rules and each profession's code of ethics.



87% of medical professionals use social media for personal purposes, which can lead to trouble if they vent about work.

Social Media Risks for Social Workers

As a social worker, you are an entity covered by HIPAA regulations, and therefore, you're held to higher privacy standards than other professions. This means you may have to maintain a delicate balancing act when using social media.

On the one hand, social media sites such as Facebook, LinkedIn, Twitter, and blogs can be formidable ways to build your credibility in the social work community and help clients. For instance, you may offer digital services such as online counseling, avatar and cyber therapy, video counseling, and self-guided web-based interventions.

On the other hand, when interacting online, you may run into issues involving...

- Privacy and confidentiality.
- Liability.
- Informed consent.
- Solicitation of clients.
- Conflicts of interest.

Let's take a look at how experts in your field use the National Association of Social Work (NASW) Code of Ethics to navigate these issues.

On Privacy & Confidentiality

Say you're assigned to a psychiatric client's case, and you discover they have been admitted because of threats of self-harm. You decide to check their Facebook page to see if they have a history of self-harm or have talked about suicide in the past. Seems professional enough, right?

According to Kathryn Chernack, the chair of the National Association of Social Workers' New York State Chapter Ethics Committee, depending on your motives, this kind of background searching actually runs against established social worker standards of practice. According to the ethics code, you're not supposed to seek out information that the patient doesn't want to share.

There are exceptions to this rule. If you work in the emergency room and you use social media searches for the patient's immediate safety or recovery, most would agree you're acting appropriately. However, if you launch the search out of curiosity, it's a violation of the patient's privacy.

This is why the NASW discourages friending or following patients on social networking sites. It's too easy to blur the lines between professional action and idle curiosity.

On Legal Liability

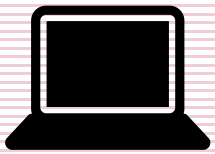
Let's say you have a young client who has a history of self-harm and has experienced abuse at the hands of their parents. If that client posts something about harm or self-harm, you could be liable if you don't report it.

The NASW reports that the Supreme Court ruled in *DeShaney v. Winnebago County Department of Social Service* that social workers can't be liable for failing to properly investigate child abuse reports. But if your relationship with the young client is established specifically for the purpose of protecting that child from abuse or negligence, you could be held liable for failing to investigate it, based on some states' rulings.

On Matters of Informed Consent

According to the NASW, psychotherapy notes have their own privacy protections under HIPAA regulations. According to privacy rules, your must obtain written client consent before you can disclose psychotherapy notes to another party. That means any notes you take during your client's session that document or analyze the conversation are strictly off-limits for sharing unless you have consent.

The exception to this rule is when the HHS or the law requires the disclosure or when disclosing the information is necessary to avert a serious and imminent threat to health or safety.



NASW discourages social workers from scoping out a client's social media profiles if they don't want to share.

That's all a given, right? You've been around this block before. But here's where questions might creep in: what if you want to write a case study about a particular client and post it on your blog?

It's a fine line you're treading, but be sure to...

- Explain the client's privacy rights under HIPAA and what information you plan to publish.
- Get consent from the client before blogging about their case.
- Redact all identifying information that could ostensibly be linked back to the client.

Read more about the NASW's ethical standards on informed consent.

On Soliciting Clients

In short, the NASW's Code of Ethics discourages the blatant solicitation of clients, and the code could be applied to how you use social media. According to Standard 4.07 [PDF]...

- Social workers should not engage in *uninvited* solicitation of potential clients who may be vulnerable to influence, manipulation, or coercion.
- Social workers should not solicit testimonials from current clients or from other people who may be vulnerable to undue influence.

It's best, then, that you don't use something a client said to market your practice on social networks and that you don't use social media as a way to fish for new clients. However, if a client reaches out to you on their own through social media and wants to know how to seek counseling through your practice, you should be within your rights to direct them to the appropriate channels.

On Conflicts of Interest

As you probably already know, the NASW Code of Ethics encourages social workers to avoid all possible conflicts of interest. In the realm of social media, that may mean...

- Encouraging online friends and family members to seek professional counsel elsewhere if they write to you with problems.
- Don't engage in business, political, or romantic relationships online with past or current clients. That may mean avoiding friend requests from clients on Facebook, Twitter, etc.

Social Media, Malpractice, and Other Repercussions

According to NASW General Counsel Carolyn Polowy, pleading ignorance about the NASW Code of Ethics won't spare you the wrath of an ethics committee if your use of social media lands you in the middle of a disciplinary proceeding.

It's also worth noting that using social media can jeopardize social workers in malpractice cases, should they arise. For example, if you exploit gray areas in the code, say, by blogging about a client without their consent, your online activity may be used against you in a malpractice claim or ethics violation hearing. It calls into question whether or not you can adequately maintain confidentiality.

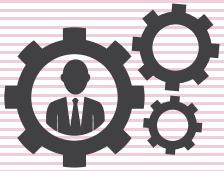
If you violate the codes, you may have your license revoked and face other disciplinary measures, depending on the case at hand.

Social workers who blog about a client's case without consent and without redacting all identifying information could get in trouble with the NASW and HIPAA regulators.

Tips for Using Social Media in Social Work

To avoid losing your social worker license and facing malpractice lawsuits, be sure to follow these tips for using social media:

- **Assume that all your social media activity is public.** Even if you delete a post or tweet, it only takes one screenshot to ensure it lives on forever in Google's endless memory.
- **Don't post about your clients.** This is especially true if you're tempted to write something negative about them or about their specific case. Confidentiality is one of the pillars of social work, and you can harm your clients' trust in your practice over a perceived breach.
- **Be professional.** Posting inflammatory comments and suggestive photographs online may harm your credibility in the field.
- **Keep your professional and personal social media accounts separate.** You might even use a pseudonym for your personal account so you can post with more anonymity.
- **Don't add clients to your social media networks.** It opens the doors for a personal relationship, which is a conflict of interest.
- **Don't use location check-ins when you're in the field.** It may inadvertently jeopardize your client's privacy.



A social worker's social media use can be used as evidence in a malpractice suit or ethics violation hearing.

Lastly, you'll want to carry Malpractice Insurance in case accidents happen. With social media constantly at our fingertips, it's easy to make a mistake in the digital age that comes back to haunt you later. Your Malpractice Insurance can...

- Cover lawsuits over professional negligence.
- Cover fines and legal defense fees related to license revocation or disciplinary proceedings.

Be sure to check with your insurance agent that your policy can adequately address your financial risks in both these instances.

Social Media Risks for Psychologists

Psychologists, when you decided to pursue your career in psychology, your studies probably led you time and time again back to one founding principle: do no harm. But with the ever-changing digital landscape in which you work, "harm" may be a loose and evolving concept.

In this section, we'll explore how the American Psychological Association's Ethical Principles of Psychologists and Code of Conduct can be applied to ethical challenges you may face when using social media. We'll also explore how you can best keep these risks at bay.

Confidentiality, Psychologists, and Social Media: A Slippery Slope

Let's start with an example lawsuit. Say you've just penned a memoir about your experiences counseling people with personality disorders. Naturally, the book is peppered with real-life cases, but you've taken care to change patient names, so you didn't ask for their consent first. Though you may think that's enough to protect your patients' identities and not run afoul of HIPAA, you are mistaken. After the book's release, a patient contacts you, recognizing their counseling session detailed in the freshly printed pages. They decide to sue you over violating their publicity rights, breach of privacy, and defamation.

Seem farfetched? Such a case happened to a doctor who treats patients for drug addiction. According to American Medical News, Michael Stein was sued by a former patient for using her case in his book without her permission, even though he changed her name.

Now consider this: when publishing a book, readers, editors, and publishers carefully vet those pages before anything is printed and distributed for public consumption. There are simply more opportunities to catch errors and double-check content before its release.

But with social media, it only takes a second to publish an anecdote about a patient. And if it's an off-the-cuff blog post or tweet, there's even less of a chance that patient consent was obtained prior to its publication.

Psychologists can be sued if they fail to get a former patient's consent before publishing details about their case, even if identifying information is redacted.

When you factor in HIPAA regulations and the APA's Ethical Principles, you can clearly see how blogging or posting about patients on social media can land your psychology practice in the crosshairs of a lawsuit.

According to the APA, psychologists are obligated to take reasonable precautions to protect confidential information. And HIPAA details 18 identifiers that medical practitioners can't include in *any* published documentation about past medical cases that a patient hasn't authorized. These identifiers include...

- Patient names.
- Geographical location.
- Dates of treatment.
- Birth date.
- Facial photograph.
- And more.

The National Center for Biotechnology Information (NCBI)'s Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research states that even with the removal of all 18 identifiers, studies found that it's still pretty easy to re-identify individuals with today's technology.

HIPAA lists 18 identifiers that can't be included in published documentation.

What Psychologists Should Know about Defamation Lawsuits

We mentioned above that breaches of confidentiality can lead to defamation lawsuits. But if you're not a legal professional, defamation may still be a big scare word that is hard to dissect.

Here's what you need to know.

Defamation occurs when someone makes a false statement about another person that causes that person some type of harm, be it emotional, reputational, or financial. According to AllLaw.com, in order to qualify as defamatory, that statement must...

- Be published (so that someone else can see it).
- Be false.
- Result in harm.

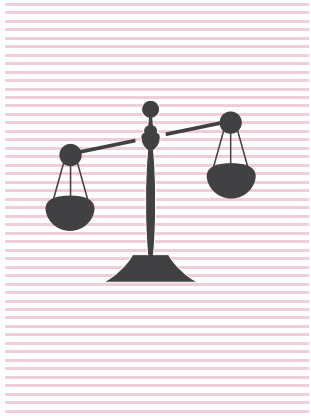
You can probably see why publishing someone's confidential mental health information on social media or blogs could cause that person reputational, financial, or emotional harm. Perhaps the patient's employer questioned whether or not to fire them because of your statements about their alleged drug abuse. But could that statement meet the other criterion of being false if what you wrote is true?

It really depends on the court that tries the case. Some could interpret your professional insights about the patient as subjective, which could be construed as false. Others may not.

As a last note on this topic, keep in mind that your General Liability Insurance can address lawsuits over advertising injuries including...

- **Libel or slander.** If you're sued over defamatory statements published on your blog or social media page, your coverage can address legal expenses.
- **Misappropriation.** You can be sued if you use someone's words, testimony, or experience to promote your practice without their consent. Though you may not be directly advertising your services, blogging about your patients could be interpreted as promoting your work.
- **Privacy violations.** Again, using a patient's case without their consent could land your practice in hot water.

Be sure to talk to an agent about getting the appropriate insurance for your psychology practice.



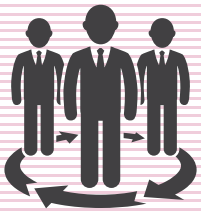
General Liability Insurance can address lawsuits over defamation and invasion of privacy.

Psychologists: How to Walk the Ethical Tightrope on Social Media

If that last section made you feel as though you should abandon your social media hopes and dreams, then chin up. There are ways to comply with HIPAA and your field's ethical codes while avoiding lawsuits. Here are some tips, courtesy of the Online Therapy Institute:

- **Maintain confidentiality.** This means all conversations should take place in private media. It's not a good idea to exchange health information via a third-party site (e.g., any social media platform) because of the limited security features. This is especially worth noting if you offer telehealth or online treatment. Only use media that offer security encryption services. The APA and Online Therapy Institute advise against friending or following patients because it can make a confidential relationship public knowledge.
- **Avoid conflicts of interest and multiple relationships.** Following or friending patients on a personal social media account can be viewed as establishing multiple relationships. Keep your work and personal accounts separate to err on the side of caution.

- **Don't solicit testimonials.** When you ask patients for reviews or testimonials, you run the risk of publicly confirming that you treated that person, which can violate their privacy rights. Plus, such a request is often viewed as taking advantage of your relationship with a vulnerable client.
- **Keep your patients informed.** Be sure to tell your patients how they can reach you in your very first session. It may also be helpful to outright discourage them from interacting with you on social media altogether by explaining that their confidential health information can be intercepted on these sites. If you search for information about your patients via search engines or social media, inform them about it. Be sure to only use this type of research in emergencies or to assist in a well-documented treatment plan that your client has consented to.
- **Minimize intrusions of privacy.** Don't publish anything about your clients or their treatment without their consent. As we discussed earlier, even redacting identifying information may not be enough to evade a defamation or invasion of privacy lawsuit. On that note, ensure that only authorized friends and followers can read your practice's social media posts. If you finish up a session and immediately use location check-in services in your post, your network may be able to identify a client's location.
- **Document and maintain records.** If you do use search engines or social media to treat patients, be sure to clearly document the circumstances for your decision. If you are ever faced with a lawsuit, these notes can help you defend yourself.



Psychologists should keep their professional and personal social media accounts separate to avoid accidentally engaging in multiple relationships with clients.

Lastly, Dr. Keely Kolmes, a psychologist, writer, and consultant, offers a social media policy that you can share with your patients. It outlines how your practice conducts itself online and how you handle interacting with clients on social media sites.

Dr. Kolmes recommends understanding social media technology before you set up a professional account. For example, some sites upload "friends" and "followers" based on your email address books, which can lead to trouble if you keep patient contacts in the same place as your personal contacts.

For more tips, check out Dr. Keely Kolmes' advice for interacting on Twitter and using Facebook as a mental health professional.

Social Media Risks for Therapists and Counselors

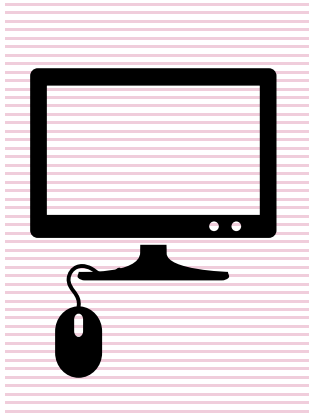
Mental health counselors – from family therapists and faith-based counselors to psychotherapists and rehabilitation counselors – may rely on social media for a number of reasons. Perhaps you offer distance therapy. Maybe you simply use it to market your practice or to swap resources with other counselors and therapists in your network. But as you now know, social media is a growing ethical gray area for mental health practitioners of all stripes.

Let's explore some common issues that could arise when you use social media in your counseling or therapy practice.

Social Media: Blurring Professional Boundaries

The American Counseling Association (ACA) Code of Ethics [PDF] recognizes that there are ways to maintain your professionalism while using social media. However, the Code of Ethics specifically prohibits personal "virtual" relationships with current counseling clients. This includes friending or following clients on social networking sites via your personal account or profile.

Does this mean you can't use social media for a professional virtual relationship? No, but you have to be careful to keep your personal and professional profiles cleanly separate. Also, it's your duty to inform your clients about your practice's social media policy and what role social media will play in their treatment. The ACA recommends that as part of the informed consent procedure, you explain the benefits, limitations, and boundaries of the use of social media.



The American Counseling Association's Code of Ethics prohibits personal virtual relationships with clients.

Now you may be asking yourself: what about past clients? Well, getting friendly with former clients can lead to personal relationships and even evolve into business or romantic relationships – both of which are frowned upon by mental health practitioner associations.

Brandt Caudill, a defense attorney who represents psychologists, psychiatrists, social workers, and other mental health professionals in malpractice cases, offers some insight on how destructive romantic relationships with past clients can be.

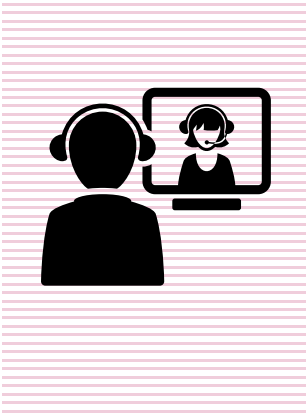
He states that even though there seems to be a rampant misconception that there's a "true love" exception where romantic relationships with clients are concerned, that's simply not true. According to most associations' ethical codes, romantic relationships are prohibited and have career-ending consequences. They are even illegal in some states (e.g., California). He advises that "under no circumstances should a therapist seriously consider a sexual relationship with a present or former patient," no matter how much time has passed.

Counselors and Therapists: Tips for Avoiding Social Media Lawsuits

You've worked hard to build your reputation as a mental health counselor or therapist. After years of schooling, experience, and fieldwork, you also know that the stakes are high for professionals who are beholden to HIPAA laws and ethical codes. One misstep online, and all your credibility could be gone. Plus, a lawsuit against your practice would make it hard to recover.

So how can you avoid getting sued over a tweet or blog you publish on social media networks?

- **Always follow the informed consent process.** As you may already know, this involves disclosing your distance counseling credentials, physical location of your practice, contact information, the risks and benefits of engaging in the use of distance counseling via online platforms, response times, and emergency procedures in your absence.



It's illegal for a counselor to have a romantic relationship with a counseling client in California.

- **Separate professional and personal social media accounts.** The ACA recommends separating professional and personal profiles. Counselors and therapists should respect the privacy of their clients' social media profiles unless they have consent to look.
- **Don't offer professional advice to those who aren't clients.** If you run a blog or use your professional social media profiles to discuss mental health issues, there's a chance that someone could seek out your advice online. It may be tempting to quickly address their question and move on, but doing so can make you liable for the outcome of that counsel.
- **Don't tweet or post status updates about difficult patients.** Of course, everyone needs an outlet. But even if you redact your patient's name, they could still be identified. Plus, HIPAA prohibits identifying treatment dates, and if you post right after a patient leaves a session, a wily lawyer may be able to argue that you inadvertently let your audience of followers know when the client in question was being treated.
- **Know that redacting identifying information may not be enough.** In the digital age, it's easier than ever to track down omitted information. If you blog about a particularly interesting client case, its uniqueness may be enough for someone on your social network to reasonably identify the client. As a workaround, some mental health professionals resort to using composite cases when blogging to better protect their patients' privacy. That brings us to the next point...

Distance therapists must be careful to follow the rules of informed consent with clients.

- **Always ask for a client's consent before using their situation as a case study.** This is doubly true if you plan to publish the study online, on a blog, or in a book.
- **Don't solicit testimonials from current clients.** Though this piece of advice may be common sense to you – current clients may, after all, be vulnerable to your influence – this is a pretty gray area where social media is concerned. For example, if you create a Facebook page for your practice and a current client "likes" that page, is it considered a tacit endorsement? Some experts in your field think so, and such an incident may call your reputation into question if you're ever sued for malpractice.

Lastly, know that there's no silver bullet for preventing malpractice lawsuits. Instead, you must do what you can to conduct yourself appropriately in any setting – in person or online – and manage risks that fall within your scope of control. So in addition to implementing these best practices while using social media, be sure you also have a safety net in place in case your best efforts aren't enough.

For instance, Malpractice Insurance can step in when your counseling or therapy practice is sued over...

- Failing to follow informed consent procedures.
- Failing to protect a client's sensitive mental health information.
- Engaging in inappropriate relationships with clients.
- Other breaches of accepted standards of care.

Your policy can help pay for legal defense fees, settlements or judgments, and other court costs, which can make the difference between your practice surviving and closing its doors for good. It can also pay for expenses and fines that accompany ethical violation hearings.

Malpractice Insurance can help pay for legal expenses if your counseling practice is sued over breaching accepted standards of care.

CHAPTER 4

OTHER TECHNOLOGICAL RISKS FOR MENTAL HEALTH PROFESSIONALS

OTHER TECHNOLOGICAL RISKS FOR MENTAL HEALTH PROFESSIONALS

Unfortunately, the risks don't end when you log off your Facebook profile or Twitter account. There's also the question of how HIPAA regulations intersect with email, text messaging, and physical technology.

It's worth noting that the laws and regulations that govern mental health professionals will always lag behind technological developments, which means what is true for professional conduct this year may not be true in five years. With that in mind, here are some other technological pitfalls to be aware of.

HIPAA, Email, and Your Mental Health Practice

As you know, it's your responsibility to ensure your patients' protected health information is secure, but whenever this data is transmitted, there's the risk that it could be exposed and your practice could be penalized for it.

HIPAA allows e-PHI to be sent over an open network as long as adequate security measures are taken.

So while HIPAA's Privacy Rule doesn't prohibit communicating with patients via email, the onus of ensuring that proper security measures are in place is on you. According to the Security Rule, you must implement policies and procedures to restrict access to and guard against unauthorized access to e-PHI. HIPAA does allow e-PHI to be sent over an electronic open network as long as it's adequately protected.

Remember, too, that under the Privacy Rule, your patients have the right to request alternate forms of communication if they are uncomfortable with email.

On Encryption

Maybe now is the time to state that HIPAA doesn't require you to encrypt e-PHI. However, the InfoSec Institute strongly advises healthcare practitioners to encrypt confidential patient information and records, especially if stored in the cloud or transmitted via email. In the event of a data breach, you don't have to notify affected parties, as long as the data is encrypted and the encryption key is safe.

At this time, HIPAA doesn't require PHI to be encrypted, even though security professionals recommend it.

Mental Health Professionals: Is Texting a Pandora's Box of HIPAA Violations?

According to the Zur Institute, texting may be the easiest way to contact young and adolescent clients, but it's not without risks.

Traditional SMS messaging platforms are typically not secure enough to transmit e-PHI. For instance, these messages can...

- Be read by people other than the intended recipient.
- Be forwarded to others.
- Remain unencrypted on telecommunication providers' servers.
- Remain on the phones of both the sender and recipient.

Having said that, there are services that offer encrypted text messaging for healthcare practitioners. If you work primarily with young clients, this may be worth exploring.

Managing Patient Records with In-Office Software

The cloud is a convenient way to store patient records, but it limits your control and oversight over the protection of your clients' e-PHI. If the cloud is hacked, you could still be held accountable for failing to properly protect e-PHI as outlined by HIPAA.

So if you manage mental health records with in-office software, be sure to...

- Limit access with passwords.
- Only allow authorized personnel to access the software.
- Create a system to record who accessed e-PHI and for what purpose.
- Use antivirus software and firewalls to keep your network secure.

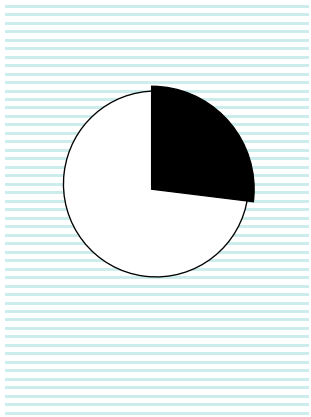
Generally, SMS messaging platforms are not secure enough to transmit e-PHI.

Physical Technology Risks for Mental Health Practitioners

Did you know that many data breaches for allied health businesses happen because of human error, such as a stolen laptop or lost thumb drive? According to a 2013 study by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association, **27 percent** of those surveyed reported that their latest data breach was caused by a misplaced portable memory device. It's another reminder to encrypt all sensitive data and not allow employees to leave the office with e-PHI saved on portable devices.

Employees who bring in their own devices to work also present risk. If they use their smartphone to connect to your secure Wi-Fi network, for example, but their device is infected with malware, your network could be at risk. Such an infection could open the door for hackers to enter your network, which is why you should always keep your antivirus software up to date.

Lastly, if you dispose of old machines or return rented ones, it's important that you have a tech expert wipe the devices first. That way, you don't have to worry about your patients' data getting into the wrong hands and being sold on the black market. (It happens.) According to Insurance Journal, your patients' health records are worth about ten times the rate of a stolen credit card because they contain complete identities.



27% of allied health data breaches were caused by a lost memory device.

What Recourse Do You Have When Your Mental Health Office Is Hacked?

The annual survey by the Ponemon Institute found that cyber attacks on healthcare organizations have increased by 100 percent in the last four years, which means it's extremely important to make your practice's data security a top priority. But first, let's recap the kind of losses you can expect if your mental health practice suffers a data breach:

- You could be fined by the US Department of Health and Human Services (HHS), which enforces HIPAA regulations.
- Your practice's reputation could be damaged.
- Your professional association could revoke your license.
- In some instances, your patients can sue you for failing to protect their privacy.

There are ways to mitigate the whopping financial consequences that accompany data breaches. Many Cyber Liability Insurance policies written for allied health professionals can help pay for these costs. For example, if your Cyber policy is industry-specific, it may...

- Pay for the cost of patching your network security.
- Cover cyber extortion expenses if your records are being held hostage.
- Fund PR measures to rebuild your practice's reputation after the breach.
- Pay for notifying affected parties about the breach (which you must do if the data isn't encrypted).
- Offer some coverage for government fines over HIPAA violations.

Many policies offer coverage regardless of whether the privacy breach was caused by a hacker's meddling or your business's honest mistake. It's important to work with an insurance agent who understands your industry so you can ensure your coverage properly addresses your data risks.

CONCLUSION

By now, we've explored the myriad ways HIPAA, social media, and other technology can lead to tricky legal and ethical territory for mental health professionals. You might feel as though you're walking a fine line when trying to educate potential clients and other practitioners about your services and experiences through social networking sites. You may wonder if anything that happens online can truly be considered secure enough for HIPAA compliance.

And you'd be right to wonder. Technology is always evolving, and with it, so are your risks. That's why if you take away anything from this guide, it should be this: stay up to date on regulations. When you aren't sure what the best course of action is, consult the endless resources offered by your industry's professional association. When you comply with what your industry states is the accepted standard of care and conduct, you reduce the likelihood of professional negligence lawsuits and other repercussions.

Lastly, be sure to stay informed about the latest technological developments that your practice may implement. HIPAA places the responsibility on you to create reasonable security practices, which means new technology may signal that it's time to revisit your risk management policies and revise accordingly.

QUICK RESOURCES

American Counseling Association (ACA) Code of Ethics

American Psychological Association's Ethical Principles of Psychologists and Code of Conduct

Clinical Social Work Association

Federation of State Medical Board (FSMB) report

Health & Human Services Summary of the HIPAA Privacy Rule

Health & Human Services Summary of the HIPAA Security Rule

HIPAA covered entities

HIPAA Title II

HIPAA's 18 identifiers

National Association of Social Work (NASW) Code of Ethics

Pew Research Center's Internet & American Life Project

QuantiaMD survery

Society of Corporate Compliance and Ethics and the Health Care Compliance Association study