

SOCIAL MEDIA USE AND MISUSE:

A GUIDE FOR PSYCHIATRISTS



Professional Risk Management Services ("PRMS") provides the information contained in this article for general use and information. Information provided is intended to improve clarity on issues regarding psychiatry services and insurance coverage, and related issues regarding those services. This information is intended, but not promised or guaranteed, to be current, complete, or up-to-date. PRMS is neither a law firm nor a provider of professional medical services, and the materials in this article do not constitute legal, medical, or regulatory advice. You should not act or rely on any legal or medical information in this article without first seeking the advice of an attorney, physician, or other appropriate professional. PRMS, The Psychiatrists' Program and the PRMS Owl are registered Trademarks of Transatlantic Holdings, Inc., a parent company of Fair American Insurance and Reinsurance Company (FAIRCO).

©2015 Professional Risk Management Services® (PRMS®). All rights reserved.

Introduction	4
Websites	5
Facebook	7
LinkedIn	10
Doximity, Sermo and Other Medically-Oriented Social Networking Communities	10
Blogging	11
Twitter	14
Listservs	15
Social Media in the Medical Office	16
Managing Your Online Reputation – Yes You Do Have One	19
Asking Patients to Rate You	20
Googling Patients	20
Physicians and Social Media – Further Guidance	22
Conclusion	23
Glossary	24

INTRODUCTION

The way patients seek out healthcare information is changing. Whereas once patients would pick up the phone and call their doctors, today's patients are more likely to look to the Internet for information. Psychiatrists are taking note of this change and are looking for guidance on using technology to enhance physician-patient communication and to provide patients with accurate and reliable information. Many are also recognizing that in order to be found by prospective patients, they need an online presence and are exploring options for achieving this.

To help in this endeavor, in the following pages we will discuss various forms of social media and ways in which they may be used by you, in your practice, and in your care of patients. And because it's what we do, we'll also discuss the associated risks of each and ways in which to mitigate those risks.

It is not our intent to discourage you from using social media but only to make you aware of areas of potential liability exposure so you may determine your own personal risk tolerance and make an educated decision as to whether it's appropriate for you and your practice. Please note also that the material provided herein is for informational purposes only and should not be construed as legal advice.

WEBSITES

One way in which physicians are utilizing social media is through the use of practice websites. Websites can range from a simple web page that is essentially an online yellow pages ad to a sophisticated interactive site. Websites have a number of important uses. They allow physicians to establish a web presence in order to be found by patients seeking treatment and to advertise their services. They can provide general practice information and streamline the appointment process by allowing patients to download history, registration, and other types of forms. Websites can also be an excellent way in which to educate patients on the conditions typically treated by a psychiatry practice and to help to screen out those who may merely be seeking drugs.

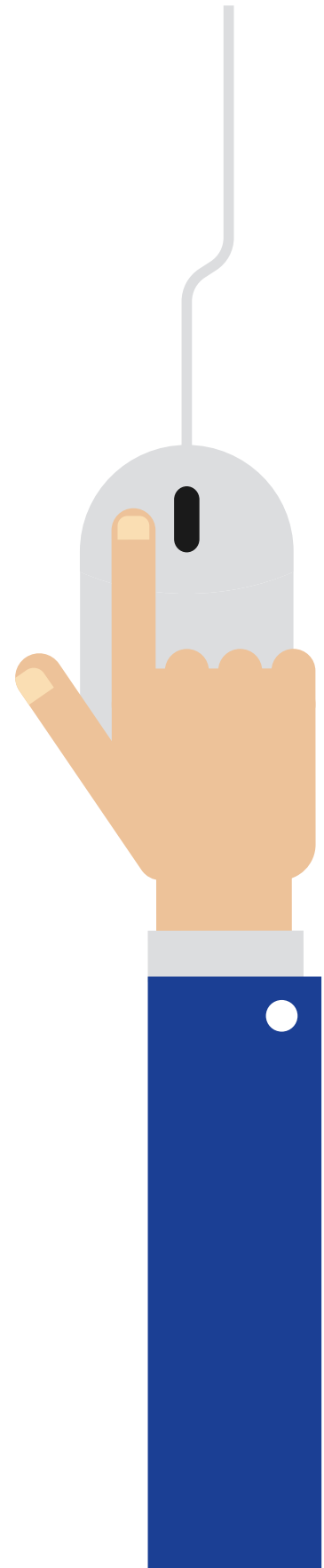
There are, however, certain considerations physicians must keep in mind when planning a practice website. **Typically speaking, the greater the interaction allowed between the patient (or prospective patient) and the practice, the greater the risk.**

One potential risk would be the inadvertent establishment of a treatment relationship. For example, if the site is interactive to the point where it allows an individual to pose a question that is then answered by a physician and the individual believes it to be treatment advice, then arguably a treatment relationship may have been established. This may be true even if the physician answering the question did not intend to establish a physician–patient relationship. It is not the intent of the physician that is relevant, but rather the “patient’s” perception.

Another potential risk is that of non-compliance with advertising and other laws (e.g., HIPAA) and ethical standards that may apply to physician websites. For example, AMA Ethics Opinion 5.02 states that physicians should not make any statements that might be misleading or construed as a guarantee of a particular result.

A third area of risk lies with information that may be included for educational purposes. First there is the potential for intellectual property violations such as copyright infringement. This may occur if information provided is the work of an author outside of the practice and authorship is not appropriately cited or credited. Specific written permission is often required before posting or redistributing information. Second is the need to ensure the accuracy of information given. Physicians must remember that they are responsible for all of the content posted on their websites thus any information posted must be accurate and up to date. AMA Ethics Opinion 5.027 provides that “Physicians responsible for the health-related content of an online site should ensure that the information is accurate, timely, reliable, and scientifically sound, and includes appropriate scientific references.”

Yet another risk lies in the potential for privacy breaches. Consider the example of the practice that opened new offices and hosted an open house for patients to welcome them to their new location. Photos were taken of the event showing patients mingling with staff and these were shared on the practice’s website. Unfortunately this was done without the permission of the patients shown which constituted a privacy breach.



RISK MANAGEMENT TIPS

- Remember that the greater the amount of interactivity allowed between the practice and individuals accessing the site, the greater the risk.
- Include a disclaimer specifically stating that the information contained on the website is not intended as treatment advice and instructing the reader to seek the care of a physician as necessary.
- Consider hiring an attorney to ensure that your website is in compliance with all state and federal laws and regulations governing physician advertising/websites.
- Obtain appropriate permissions before using materials from other sources. If linking to other websites, link only to credible sites and first review the information for accuracy. Periodically check to see whether the links are still live. You may also wish to include a disclaimer stating that you are not responsible for the information contained on those links keeping in mind however, obligations under AMA Ethics Opinion 5.027.
- Remember not to make any statement on your website that might be construed as a guarantee of a particular treatment result.
- If you are selling products on your website, ensure compliance with applicable laws and ethics standards.
- Never post patient photos, comments, etc. without the patient's consent.
- Limit the staff members who may post to the website and have a second person check for errors before posting.
- Do not allow non-patients to communicate with you via the website to avoid the inadvertent establishment of a treatment relationship. Current patients should communicate via a secure patient portal only.
- If prospective patients can download forms, consider including a statement that doing so does not guarantee that a treatment relationship will be established.
- If you have online appointment scheduling via your website, ensure that all information is secure and not available for others to see. One practice learned this lesson the hard way after having to pay \$100,000 to stop the government investigation resulting from a publicly accessible online scheduling calendar containing patient demographic and medical information.

FACEBOOK

In March of 2009 there were 56,769,060 Facebook users. By March of 2010 that number had more than doubled to 114,190,780. At the time this article went to press, there were more 1.49 billion monthly active users. It's no surprise then that included in this 1.49 billion are a significant number of physicians.

Many physicians have found Facebook (and other similar sites) to be an easy way to stay current with friends and family despite their hectic work schedules and dearth of free time. A number of professional organizations, including the APA, maintain Facebook pages thus allowing physicians to keep up with colleagues and professional developments as well. All of this sounds like a good thing for all involved, so what's the downside?

Even though you may be operating a Facebook or other social media page for your personal use only, you cannot assume that this can be kept completely separate from your professional life. While you may be able to control who sees what you post on your own wall, you cannot control who sees what you post on the walls of others nor can you control what is reposted from your wall. Even among approved friends, there is always the possibility that a post will be made on your wall (or that you may be "tagged" in a post) that could cause embarrassment or have a negative impact upon your professional life.

Before joining a social networking site, you should understand that everything you post:

- ⊕ Will always be out there somewhere – even if it has been deleted. Every conversation is recorded electronically and may resurface at a later date where it may be taken out of context and present you in an unflattering light.
- ⊕ May be viewed by patients – even if you have not "friended" them.
- ⊕ May be viewed by your employer or your staff.
- ⊕ May be viewed by professional colleagues or prospective employers. Recruiters are looking more closely at candidates and this scrutiny is often extended to Facebook and other social pages. While a photo of you enjoying a drink with a group of friends or the inclusion of profanity may not preclude you from getting a job, they can tip the scales if the competition is tight.
- ⊕ May be viewed by your professional licensing board. One Rhode Island physician was reprimanded by her Medical Board after she posted sufficient information about a patient to allow that person to be identified by others.
- ⊕ May be accessed by a plaintiff attorney and admissible in court in a lawsuit against you. Imagine being faced with the following questions in court: "What else was going on with you the night you failed to diagnose the? Were you busy posting comments and photos on your FB pages? Had you been out with partying with friends while on call?"

In *Romano v. Steelcase Inc.*, 2010 N.Y. Misc. LEXIS 4538 (N.Y. Sup. Ct. Sept. 21, 2010), the judge ruled that the defendant was entitled to access the plaintiff's current and historical Facebook and MySpace pages and accounts – including previously deleted information on the basis that information found there could prove to be inconsistent with her claims of loss of enjoyment of life after she'd been injured falling off a defective chair manufactured by the defendant.

The judge granted the defendant's request for discovery because the primary purpose of social networking sites is to "enable people to share information about how they lead their social lives." While in this instance, this information was used to discredit the claims of a plaintiff and to mitigate her claimed injuries, it is just as likely that such information might be accessed and used against a defendant psychiatrist.

Another concern is the inadvertent establishment of a treatment relationship. If someone poses a medical question (even if on your purely personal site) and you answer it by giving specific treatment advice, you may have established a treatment relationship with the documentation to prove it. Further, if this friend is not located in a state where you hold a medical license, you may be deemed to be practicing without a license which is a crime in many states. To add insult to injury, if your friend follows your advice and has a bad outcome and files a lawsuit, your liability carrier may not cover you as you were practicing without a license.

Friending Patients

A friend request from a patient can be a complicated thing. Psychiatrists are required to maintain absolute boundaries and are expected to maintain a professional distance from their patients. The AMA Social Media Policy discourages physicians from socially interacting with patients, as does the Federation of State Medical Boards in its Model Policy Guidelines for the Appropriate Use of Social Media and Social in Medical Practice.

In the event that a patient sends you a friend request, our risk management advice is to politely explain to the patient that although you are flattered by their request, you prefer to keep your private life private. It is, however, appropriate to discuss the implications of the friend request. If your practice has its own page, you may wish to direct patients there.



“There is always the possibility that a post will be made on your wall (or that you may be “tagged” in a post) that could cause embarrassment or have a negative impact upon your professional life.”

RISK MANAGEMENT TIPS

- Do not blend personal and professional pages.
- Maintain strict privacy controls on personal pages.
 - Do not allow personal pages to be visible on search engines.
 - Limit who may see whom you have friended – patients may look to their pages for additional information about you.
 - Do not allow access to your photos by anyone other than friends.
 - Set privacy controls so that you must give permission before you are tagged in someone else's photo.
- Do not use an actual photo of yourself as a profile picture.
- Test your settings by having someone who is not a Facebook friend access your homepage. Click next to your name in the search box to see what photos of you or comments you've made are accessible to others.
- Remember, if you post on the wall of another Facebook member with different privacy settings, your post may be visible on search engines.
- Make sure your children, friends, and significant others understand the need for you to maintain a professional image and ask them not to post information about you or tag your photos without your permission. Ideally they too will utilize strong privacy controls.
- If you are not on the site often enough to monitor your page, consider taking it down.



LINKEDIN

LinkedIn is a free professional networking site for the business community with over 380 million members worldwide that allows members to establish a profile with their education, work information, publications, etc. – much like an online curriculum vitae. Members may link to other members and follow companies and topics of interest. An important benefit for physicians is that it scores very high on a Google search meaning that if someone were to Google your name, your LinkedIn page would be listed before review sites, thus allowing you to control the information a patient or prospective patient first learns about you.

RISK MANAGEMENT TIPS

- Do make certain your profile reflects the image you would want to project to your patients.
- Just as with Facebook, do not connect with patients.

DOXIMITY, SERMO AND OTHER MEDICALLY-ORIENTED SOCIAL NETWORKING COMMUNITIES

Whereas once physicians could stay current with medical developments by reading medical journals and attending conferences, the amount of information currently available makes it impossible for any one physician to stay on top of all of it on his own. Accordingly, physicians are looking for ways to efficiently monitor and manage the overabundance of information available to them and are turning to sites such as Doximity and Sermo to help with that. Doximity and Sermo are online physician communities, the purpose of which is to allow physicians to collaborate on difficult cases and to share observations and information on various drugs, devices and issues ranging from patient care to practice management.

Open to physicians only, one feature of these sites is a social media version of the traditional curbside consult. However, unlike the curbside consult, here there is left a permanent record of the exchange – a record that could conceivably be misdirected and result in a violation of patient privacy. Even though these sites may be limited to physicians only and one would expect that everyone accessing information would comply with medical ethics and professionalism, users should be aware of potential problems.

RISK MANAGEMENT TIPS

- Always operate under the assumption that the information will be made public and include as few identifying details as possible.
- Be aware that others posing as physicians (or plaintiff attorneys who are MD/JDs) may try to access information.
- Consider whether the benefit of this type of consultation outweighs the potential for a privacy breach. In other words, what is the likelihood that you will obtain better information there than you would from a local colleague?
- If a local colleague is not available, consider whether a secure email to one known user is a safer option.

BLOGGING

It is no secret that blogs, or journal-style websites whose authors publish content over time, are becoming increasingly prevalent. A 2008 article in the *Journal of General Internal Medicine* (J Gen Inter Med 23(10):1642-6) reported the results of a study that found an estimated 70 million blogs then in existence, with over 100,000 new blogs being created every day. Blogs can be whatever their authors want them to be, from a stream-of-consciousness rambling to a well-planned repository of educational information on an identified subject.

Although it is difficult to estimate how many physicians have or contribute to blogs, it is likely a significant number. As with all other tools utilized in medicine, any person using or contributing to one should carefully evaluate why and how it is being used and whether it is appropriate to do so in light of professional obligations and aspirations. Accordingly, healthcare-related blogs should be carefully crafted to further legitimate healthcare goals and comply with physicians' professional responsibilities.

To illustrate, in the above-referenced study from the *Journal of General Internal Medicine*, it was noted that, of 271 medical blogs reviewed, three posted identifiable photos of patients. The study report also gave examples of other postings on blogs written by healthcare professionals that were decidedly less than professional. One doctor wrote on his blog of a patient that "she was a stupid, lazy, selfish woman all of which characteristics are personal problems, not medical issues or barriers to care."

Anonymity is no justification for breaching professional ethics. Moreover, contrary to what doctors may think, blogs purporting to be anonymous may not actually be anonymous; the same study found that over 55 percent of "anonymous" blog authors provided enough information to reveal their identities.

Whether a blog is intended for personal or professional use, another consideration is the potential for inappropriate self-disclosure. In other words, is there personal information contained within the blog which, if read by patients, employees, or employers, would negatively affect the physician's professional image? Remember, anonymity is rarely absolute and physicians should assume that even anonymous, personal blogs will be discovered by intrepid patients proficient in the use of search technologies.

In sum, blogs can be useful communication tools; however, physicians should assume that everything written there will be found by patients, employers, employees, and the opposing side in an administrative or legal action. Physicians should carefully consider the goal of the blog and whether they can contribute content in a manner that comports with their professional responsibilities.



RISK MANAGEMENT TIPS

CONFIDENTIALITY

- Patient information must be kept confidential. There is more to de-identifying information than deleting a name.
- Consequences for breaches in confidentiality may include: discipline by your licensing board, a civil lawsuit, and governmental enforcement action (such as by OCR, the federal agency responsible for enforcing HIPAA's privacy and security rules).
- Advise readers that details have been changed to protect your patient's privacy. If certain identifying details – age, race, gender, etc. – are important to retain the value of your post, and the possibility exists that the patient (or someone who knows the patient) would be able to identify the patient, ask the patient's permission to share his story and obtain written permission to do so.
- As part of the consent process, patients should be made to understand that once the information is online, it is out there forever. Patients should also be prepared for the possibility that comments might be made regarding the post that might be unpleasant to them.

PUBLIC FORUMS

- Be aware that you are responsible for all content that you publish and if you have your own blog, everything that appears on it. Carefully consider the permissions you will give others with regard to posting content or comments. Ideally no one but you should be able to publish posts on your blog or write comments that appear on your blog. Your blog is not only a reflection of you but of the entire medical profession. Use your blog to educate not to vent about patients or colleagues.
- If others are allowed to write on your blog, be sure that you can and will review all writings before they appear and that they are not misleading and do not violate any of your ethical or legal obligations. Because you are responsible for all content, it must meet the standards to which you yourself are held. Thus, even non-physician contributors should not be allowed to engage in such activities as publishing patient information on your blog.
- Readers (and regulatory bodies, licensing boards, etc.) expect a high level of integrity and accuracy from physicians. Use the same standards for disclosure and ethics that you would if publishing for a professional journal. If you intend to present a fictional story, that should be made clear to your readers. AMA Ethics Opinion 5.027 states, "Physicians responsible for the health-related content of an online site should ensure that the information is accurate, timely, reliable and scientifically sound, and includes appropriate scientific references."
- AMA Ethics Opinion 5.027 also discusses conflicts of interest. Generally, any potential conflicts should be disclosed.
- Never insult another physician or patient. Never say anything online that you would not be comfortable saying in front of a group of your most esteemed colleagues.

PHYSICIAN ANONYMITY

- If you are blogging under a pseudonym, do not assume you are anonymous even if you have taken steps to disguise your identity. Because blogs are accessible to such a large population, the ways in which your identity may be discovered increase exponentially and the amount of detail required for someone to identify you accordingly decreases exponentially.

RISK MANAGEMENT TIPS (CONT'D)

TREATMENT RELATIONSHIPS

- Avoid inadvertently creating a treatment relationship with your readers. Keep in mind that it is the perception of the reader that matters, not your intent. Make it clear that no treatment relationship exists, do not post anything that could be perceived as a treatment recommendation, and clarify that nothing on the site is intended as medical advice.
- Publishing general educational information about a disease or treatment is not usually viewed from a legal perspective as being medical advice; however, making suggestions to a person regarding his or her diagnosis or treatment will almost always be viewed as medical advice and may be sufficient to establish a treatment relationship.

SELF-DISCLOSURE

- Because blogs are public forums and anonymity cannot be assumed to be absolute. You should assume that intrepid patients will find even anonymous personal blogs and postings.
- Be aware of the implications a blog or postings may have for your professional relationships. For example, would you be comfortable with your patients, employees and employers seeing what you post online?
- If you have both a personal and professional site, the safest approach is to keep them completely separate but to approach the content in the same manner.

DISCOVERABILITY

- Information posted is discoverable in litigation. Just as statements made in journal articles or depositions given in legal proceedings, comments made by you in your blog may be used to discredit you should you be named as a defendant or called as a witness in a lawsuit.
- Flea was a Massachusetts pediatrician who blogged at length about the malpractice trial in which he was the defendant. He ridiculed the plaintiff's case and the plaintiff's attorney, revealed the defense strategy and accused jurors of dozing. Unbeknownst to him, the plaintiff's attorney was aware of this and during her examination of him, she asked the doctor if he was Flea. The case settled the next day for an undisclosed amount.

ADVERTISING

- Be aware that advertising rules generally apply to websites, including blogs. Many free blogging platforms are ad-supported and some do not allow the user to control which ads appear on his or her site. Some bloggers use their site as a platform to advertise or endorse products.
- Be familiar with state and federal laws governing physician advertising as well as any rules promulgated by your state's medical board.
- Potentially relevant ethics guidelines to consider include AMA's E-502 (Advertising and Publicity), E-8.062 (Sale of non-health related goods), E-8.063 (sale of health related goods).

TWITTER

Twitter is a microblogging network that allows its users to send and receive messages of up to 140 characters which are known as tweets. Contained within tweets may be hyperlinks to other media such as websites or individual articles. Hashtags may be added to allow readers to search tweets by a particular topic. While one might at first think that such limited space would not allow for effective communication in a medical context, in fact there are numerous ways in which twitter has been used by the medical profession.

- + An extension of their web presence
- + A patient communication site for:
 - + Practice updates
 - + Alerting patients to relevant health-related articles
 - + Real-time updates when MD is running behind
- + Marketing tool
- + Virtual water cooler with colleagues
- + Staying current on professional information
- + Mechanism for real-time questions/commentary during conferences
- + Networking
- + General education for the masses
- + Provide reliable info during public health emergencies, e.g., H1N1

The timing of tweets may be subject to scrutiny both by patients and plaintiff attorneys. The patient who's been sitting in your waiting room for an hour does not want to receive a tweet from you even if the information presented is relevant to them. The tweets you sent from home one evening may come back to haunt you when the fact that you determined you did not need to come in and see the patient in response to the call from the ER physician is later called into question.

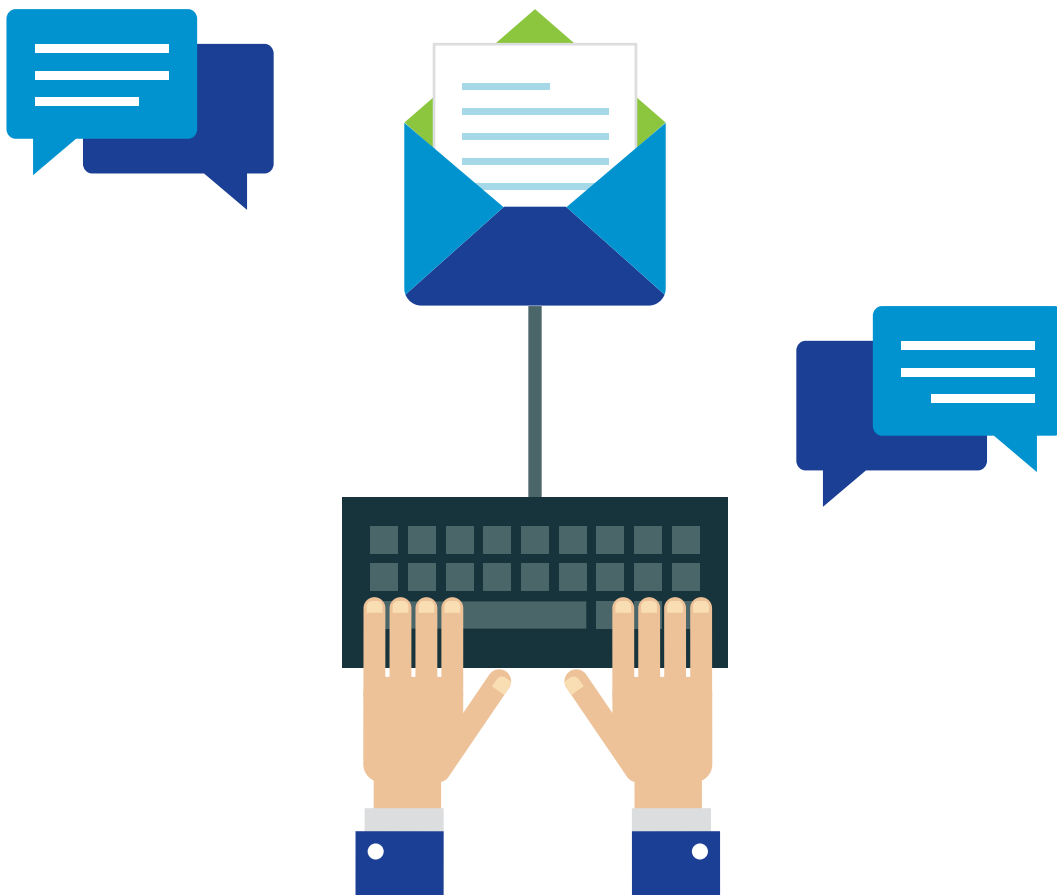
RISK MANAGEMENT TIPS

- Twitter is really a microblog and thus the risk management advice associated with blogging should also be followed.
- Avoid tweets that are derogatory or would reflect poorly on you as a physician.
- The timing of tweets is recorded and could potentially be used against a physician in litigation if there is a question that he/she was distracted or failed to respond to a situation.
- Depending upon your purpose for utilizing Twitter, you may wish to keep your tweets private.

LISTSERVS

Listservs are an excellent way to share information between large groups of people. Individuals who wish to receive updates on a particular topic can join the listserv to receive information and also participate in discussions. Problems arise, however, when these discussions involve issues of patient care. In order to avoid potential liability exposure, keep these points in mind:

- + Patient confidentiality must be maintained and this requires more than simply removing the patient's name.
- + Although listserv membership may be granted to only a small select group, comments can be forwarded to anyone and everyone – including plaintiff attorneys.
- + Listserv entries may be discoverable in the event of litigation. This could apply both to the original poster as well as those commenting in response. One of the first questions a plaintiff attorney will ask of a defendant physician is with whom he/she discussed the patient's treatment. Those named will likely be questioned.
- + Efforts should be made to frame patient care discussions only as a type of informal consultation rather than as specific treatment advice. True consultations (no prescribing, no written orders) are generally relatively low risk activities because the one requesting the consult is free to accept or reject the consultant's thoughts. Avoiding the appearance of treatment advice will be more difficult when discussing cases with non-physicians. If non-physician practitioners are asking for advice from physicians on a listserv, they may be seen as less able to choose to ignore the advice of the physician – and from a liability perspective, the arrangement could look more like supervision than consultation.



SOCIAL MEDIA IN THE MEDICAL OFFICE

Some psychiatrists have developed pages for their practices as a source of advertisement and a mechanism by which to educate patients. Patients may also have the ability to “friend” the practice. Keep in mind however, that unless you are careful, confidentiality may be easily breached. The names of those who are friends of the practice may be visible to other friends. Even this simple fact is a HIPAA violation. As with websites, never include pictures of patients without their actual written consent.

RISK MANAGEMENT TIPS

- Set privacy controls so that the names of those who are following the practice are not visible.
- Never post photos of patients without their written consent.
- Be aware that Facebook may create an unofficial page for your practice if you have not created one. If you become aware that this has occurred, ask Facebook to remove it. If they will not, alert patients to the fact that anything they post will not be private.
- Do not allow patients to post comments on your page.

Physicians should also be aware of potential liability exposure to their practices through the misuse of social media by employees – both inside and outside of the workplace. Recent headlines regarding inappropriate postings have demonstrated a lack of knowledge among healthcare workers as to what constitutes confidential patient information, which in turn has resulted in reputational damage to physician practices along with board complaints, regulatory fines, and litigation.

As demonstrated by a Michigan case, inappropriate social media disclosures often demonstrate an ignorance or misunderstanding of privacy laws. In this case, a hospital employee posted her feelings on Facebook following a particularly emotional night in the emergency room treating both a police officer who was shot and the shooting suspect. She was surprised to be reprimanded and fired for violating HIPAA regulations after she wrote that she had come “face-to-face with a cop killer and hoped he rotted in hell.” Following her termination, she voiced her confusion as to why she had been terminated: “I am familiar with HIPAA. I did not give out any of his information. I did not give out his name. I did not mention the hospital. I did not give out his condition.”

This hospital employee is not alone. Many healthcare workers erroneously believe that by omitting the patient’s name or other identifying information when posting information, they have sufficiently protected patient privacy. Others believe that posting information to a social media site from home, rather than from the workplace, entitles them to share the information without any repercussions.

One way to eliminate such misconceptions is through the use of an office social media policy. A comprehensive social media policy can help to insulate the practice from potential liability exposure and create an environment that protects the privacy of all patient information. While it may seem that the best solution is to simply forbid access to social networking sites from office computers, this may not be sufficient as employees can still obtain access through personal mobile devices and from home after hours. Even if an individual claiming breach cannot establish a claim of vicarious liability, bad publicity can still negatively impact the practice. Thus, developing organizational policies regarding the use of social media inside and outside of the workplace and providing comprehensive training on such policies is an important step in limiting a practice’s liability exposure.

Creating a Social Media Policy

The first step to drafting a comprehensive social media policy is to understand the role played by social media within your practice, through your employees and your patients, personally and professionally. Consider implementing an internal audit to discover how social media is being utilized by employees and patients in your practice, both formally and informally. The results of such an audit will provide crucial information to developing a comprehensive social media policy. Next, consider the vision, mission and goals of your practice in relation to social media such as the type of image you seek to create in the public and the overall goals that you seek to accomplish through the use of social media. This will provide a framework for outlining the permissive use of social media, as well as the specific individuals who should be responsible for monitoring and developing the content delivered through social media. In this process, it's important to consider the various ways in which social media can be used by the practice, such as by employees while inside and outside the workplace, with respect to services and products provided or by you during the recruiting and hiring process.

Participation in social media creates numerous legal liability exposures within diverse areas of the law, with the potential to incite causes of action for trademark and copyright infringement, defamation, endorsements, violation of privacy and publicity rights and labor and employment regulations. The exposure increases significantly in the context of healthcare organizations, which are subject to additional and far more stringent regulations, such as HIPAA, state health information privacy laws, federal and state fraud and abuse statutes, standard of care requirements, and the nuanced issues that come to light with the ubiquitous nature of social media, such as inadvertent creation of the physician-patient relationship and the unlicensed practice of medicine. Most importantly, litigation involving such issues becomes infinitely more complex, as the content on social media sites is permanent and discoverable by courts and written communication, such as emails, Facebook posts or comments and tweets, can be easily misconstrued, particularly content drafted for the purposes of social media, which is often written without much forethought.

The National Labor Relations Board has taken an active role in protecting employee use of social media, which should be taken into consideration when drafting and implementing a policy, as the NLRB will deem unlawful any social media or confidentiality policy that employees could “reasonably interpret to prohibit protected activity,” such as broad provisions requiring discussions to be appropriate, respectful, professional or those prohibiting disparaging and inflammatory comments. Therefore, organizations should be cautious when restricting employee conduct, particularly with the use of generic or overly broad provisions that may be construed as restricting an employee’s right to publicly criticize their employer or discuss the terms and conditions of their employment. Encouraging employees to refrain from disparaging language is allowed, but employers should not impose provisions that are written as “absolutes,” as it is these provisions that have been held by the NLRB to be unlawful.ⁱⁱⁱ



“The content on social media sites is permanent and discoverable by courts, and written communication, such as emails, Facebook posts or comments and tweets, can be easily misconstrued.”

Elements of a Social Media Policy

The following are suggested elements to be included in an office social media policy, which should be modified and expanded upon to meet your needs as appropriate:

Purpose/Objective of the Policy

Clearly establish the objective of the policy and the role it will play within your practice. Emphasize that the policy governs both the use of social media at the place of employment and personal use of social media.

Prohibited Uses

This section should outline specific uses that would not be allowed via practice-hosted social media or personal social media, including:

- ✔ Posting false, obscene, harassing statements or statements disparaging an individual's race, religion, age, sex or disability.
- ✔ Posting of any patient information or photographs.
- ✔ Disclosure of the practice's financial, proprietary, or other confidential information.
- ✔ Utilizing practice trademarks or logos on personal social media.

This section can also feature hypothetical scenarios based closely on real-life case examples. This will allow employees to become familiar with the uses that are not allowed and the possible sanctions that can result from such use of social media.

Social Media Best Practices/Permitted Uses

By outlining the type of uses that would be permitted under the policy, you can further decrease the likelihood of an employee violation and delineate the boundaries for the use of social media.

- ✔ Encourage employees to utilize citations whenever possible to prevent copyright and intellectual property issues.
- ✔ Encourage employees to include disclaimer as to medical advice when posting educational information.
- ✔ Encourage employees to include disclaimer that posts by others not affiliated with the organization are not attributable to the practice.
- ✔ Encourage employees to post photos of coworkers only if taken outside of work and only with the coworker's permission.
- ✔ Specify that employees are not to speak for the practice on social networking sites or blogs, only for themselves.
- ✔ Ensure that employees understand that content posted on social media is easily misconstrued, permanent, discoverable and can be utilized in adversarial proceedings.

Violations and Enforcement

Specify the sanctions that would result if an employee violates the policy.

Protected Activity by the National Labor Relations Board

The NLRB has been active in protecting employee use of social media who engage in concerted activity for their mutual aid or protection. This includes allow employees leeway to express their views in a manner that employers may consider rude, discourteous and/or disloyal.

Explicitly state that the policy is not intended to interfere with protected activity as defined by the NLRB or infringe upon employees' rights.

Employee Affirmation/Acknowledgement

This concluding section should require an employee to confirm through his or her signature that the employee understands and agrees to abide by the policy.

MANAGING YOUR ONLINE REPUTATION – YES YOU DO HAVE ONE

Even if you have never even accessed the Internet, there is no doubt that you have an online presence. If there is an “M.D.” or “D.O.” after your name, you can rest assured that someone, somewhere will have posted information about you. Perhaps it is your business contact information or the fact that you attended a conference, or a link to an article you published. On the other hand, it could be that embarrassing photo of you from medical school that a friend posted on her Facebook page or a negative review from a disgruntled patient. In any case, it is important that you know what is posted about you so that you can take necessary steps to protect your reputation:

- + Start by googling your name in all of its possible derivations: John Smith, John Smith, MD, John K. Smith, John K. Smith, MD, etc. Look not only for written content but for images as well.
- + Set up a search alert. Google will allow you to set up alerts so that you receive email notifications whenever Google finds that someone has posted content about you on the Web.

Certainly if friends have posted embarrassing personal information, photos, etc., you will want to ask that they be removed. It is more difficult to deal with negative reviews but you are not powerless. Some ideas to consider:

- + If you can identify the patient, you may wish to contact her to see whether any problems can be resolved which would then cause the patient to reconsider her review.
- + If you believe the information to be false, contact the company posting the review and ask that it be removed.
- + Remember that just because a patient posts information about your care online it does not mean that she has waived confidentiality. Do not attempt to counter a bad review by posting your version of the care rendered.
- + If a negative review misstates a fact about policies or procedures within your office, you may clarify this on your website. For example, if a review states that a patient was told he'd be given a prescription at his first visit but was not, you could state on your practice website, “It is my policy not to provide prescriptions at the first appointment.” You may not however in any way reference the complaint made by the patient.
- + Beware of companies that charge you to manage your online reputation. It is unlikely that they can do anything that you yourself could not do with a little time and know-how.
- + Do NOT try to prevent bad reviews by requiring patients to sign contracts wherein you promise to maintain their confidentiality if they in turn promise not to post a bad review.
- + Do not attempt to counter negative reviews by posting fake positive reviews. This practice is called “astroturfing.” One physician practice was fined \$300,000 after the state Attorney General learned that staff members were posing as patients and writing glowing reviews in an effort to mitigate the poor reviews of real patients.
- + Set up a LinkedIn page or a simple practice website. That way, when someone Googles your name, one of the first “hits” they will see will be information provided by you.

ASKING PATIENTS TO RATE YOU

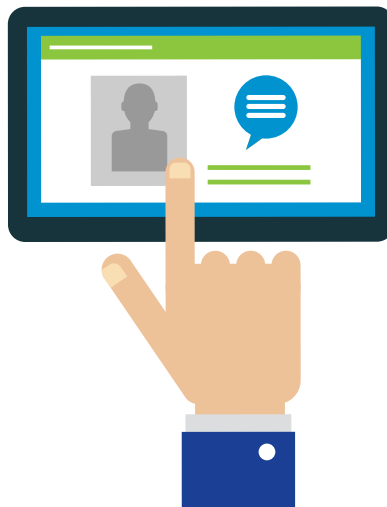
Asking patients to rate you sounds like a perfectly logical thing to do. After all, you have literally hundreds of satisfied patients – why shouldn't their opinions be heard as opposed to those of a handful of crazy drug-seekers? And while many may be more than happy to do so, you should exercise extreme caution when soliciting patient testimonials. Carefully consider the position of your patients and the fact that some of them may not feel as though they can refuse your request.

If a patient has provided you with a positive review and you wish to use this review say for example by posting it on your website as a testimonial, remember that you must have the patient's permission to do so. Also, per the AMA Ethics Opinion 5.02 Advertising and Publicity, "generalized statements of satisfaction with a physician's services may be made if they are representative of the experiences of that physician's patients."

GOOGLING PATIENTS

We've discussed the importance of not engaging with patients on social media but now let's consider for a moment how social media might actually impact the treatment of patients. What started out simply as the name of an Internet search engine, "Google" has now become an everyday part of our lexicon as well as our lives. It is no longer necessary to spend time trying to remember mundane facts or to go to a library to obtain information. One need only grab the nearest Internet-enabled device and "Google it" to find more information about any topic than anyone could possibly ever want.

This ease in obtaining information can, however, prove a dilemma to physicians in general – and to psychiatrists in particular – when it comes to the question of whether this ease in access to information should also extend to information regarding patients. What only a few years ago would have been considered confidential (and arguably off limits) is now available to the general public – much of it having been posted by the individuals themselves. If the whole world can access a patient's information, shouldn't his or her psychiatrist have it as well? Should a psychiatrist Google his or her patient?



Before performing a search on your patient, consider the following:

What is my purpose for this? If you have a legitimate treatment purpose, e.g., a third party has informed you that a patient has been posting thoughts of suicidal or homicidal ideation on his blog, proceed but with caution. If your purpose is more along the lines of curiosity, step away from the keyboard – fast!

What specific information am I looking for? Take care in defining your search terms to help ensure that you have a legitimate purpose for viewing the information returned.

Should I first obtain my patient's permission? Absent a safety issue that requires an urgent response, advising your patient of your desire to obtain information and asking their permission to do so helps to maintain the patient's trust.

Should I access the information only in the presence of my patient? This may depend upon the nature of the information. For example, if your patient was the victim of a heinous crime and you believe knowing more about the incident will better help you treat your patient, you should consider the impact revisiting this information would have upon the patient.

What will I do if I find out information that is offensive to me and causes me to think less of my patient as a person? What if I learn that my patient has filed multiple lawsuits against previous physicians? What if I learn that my patient who won't pay my fees comes from a very wealthy family? What if I see that my patient is engaging in activities I may be required to report? What if I see my patient who is claiming disability engaging in extreme physical activity? Before hitting "search" you have to be prepared for what you might find. Avoiding some of the information may be possible by using narrow search terms as discussed above and exercising extreme willpower. But you may still stumble across information that would make you uncomfortable and you must consider how this would impact your treatment relationship.

How do I know the information I uncover is reliable? Does it appear to be from a credible source? Is it current information?

Will I need to print out the information and put it in the patient's chart? If it is information that was relied upon in making treatment decisions, arguably yes. Remember that whatever is placed in the chart becomes a part of the patient's permanent record and must be released whenever records are requested. This supports the idea of gaining the patient's consent before accessing information.

Can accessing this information increase my liability exposure? For example, what if, with your patient's knowledge, you are reading his blog and after months of relatively benign entries, you decide to skip a few weeks and thus don't notice when your patient outlines a plan to commit suicide which he then implements? Have you imposed a greater duty upon yourself when you undertook monitoring your patient's web activities? Possibly so.

RISK MANAGEMENT TIP



Googling patients opens a Pandora's box of ethical and liability issues. As noted in the APA's Opinions of the Ethics Committee on The Principles of Medical Ethics, 2014 edition, while Googling a patient isn't unethical, it should be done only for the purpose of promoting patient care. Accordingly, our conservative risk management advice is that, unless presented with a compelling and/or urgent need to obtain information for the purpose of treatment or safety of the patient or others, Googling patients is best avoided.

PHYSICIANS AND SOCIAL MEDIA – FURTHER GUIDANCE

State licensing boards are reporting that they are receiving complaints related to physicians' use of social media. Not only are boards investigating these complaints, they are in some cases imposing serious disciplinary action. The boards are indicating an interest in regulating this practice and may enact guidelines or regulations based on, in part or in whole, the Federation of State Medical Boards in its Model Policy Guidelines for the Appropriate Use of Social Media and Social in Medical Practice.

RISK MANAGEMENT TIPS

- ➔ Appropriate use of social media within the office should be addressed as part of your regular HIPAA training of staff.
- ➔ Review the Federation of State Medical Board's (FSMB) Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice.
- ➔ Establish a social media policy within your office regarding appropriate content for all media used – websites, blogs, Twitter, etc. Policies should be straightforward and rigorously enforced.
- ➔ Require that posts on business-hosted blogs and twitter accounts be made by only one person or a select few. It is recommended that posts be proofread by an appointed person prior to posting.

State Licensing Boards Are Looking at Physicians' Use of Social Media

Pursuant to the AMA's policy on the use of social media, psychiatrists should:

- +
 - +
 - +
 - +
 - +
 - +
 - +
 - +
- Be cognizant of standards for patient privacy and confidentiality and refrain from posting identifiable patient information online.
 - Utilize privacy settings and routinely monitor their own internet presence to ensure information posted is accurate and appropriate.
 - Maintain appropriate professional boundaries with patients.
 - Consider separating personal and professional content online.
 - Bring to the attention of colleagues content on their sites that is inappropriate.
 - Recognize that online activities may negatively affect their reputations among colleagues and patients and undermine trust in the profession.

CONCLUSION

At this juncture, we simply do not know all of the liability issues that may arise from the use of the Internet and how these will play out in the courts. At a minimum, however, we can assume that risks will be the same as they are for activities conducted off-line. Technology can have a very positive impact on efficiency and the practice of medicine. However, physicians must understand that technology does not change their obligation to meet clinical, legal, and ethical standards. As such, physicians engaging in technology must remain mindful of the associated risks. Your decision to engage in these activities will be based upon your individual practice, your patients, and your own personal tolerance for risk.

REFERENCES

Yin, Sandra. Hospital Worker Fired over Facebook Comments about patient. August 1, 2010. Fierce Healthcare. <http://www.fiercehealthcare.com/story/hospital-worker-fired-over-facebook-comments-about-patient/2010-08-01#ixzz246V2QxHv>

³Acting General Counsel releases report on employer social media policies. National Labor Relations Board. May 30, 2012. <http://www.nlrb.gov/news-outreach/news-releases/acting-general-counsel-releases-report-employer-social-media-policies>.

⁴OFFICE OF THE GENERAL COUNSEL. Division of Operations-Management. MEMORANDUM OM 12-31 January 24, 2012. Page 4. "The Employer's rule prohibited "[m]aking disparaging comments about the company through any media, including online blogs, other electronic media or through the media." We concluded that this rule was unlawful because it would reasonably be construed to restrict Section 7 activity, such as statements that the Employer is, for example, not treating employees fairly or paying them sufficiently. Further, the rule contained no limiting language that would clarify to employees that the rule does not restrict Section 7 rights."

GLOSSARY

ASTROTURFING

The attempt to create the impression that there is widespread grassroots support for a particular policy, product, or individual where in reality no such support exists. This is done through creating multiple online identities aimed at misleading the public, making them believe the position of the astroturfer is commonly held. This can be done by a single person creating multiple identities online to review a product, giving the unknowing public the idea that the product is highly-used and well-liked by its users.

BLOGGING

A diary or commentary maintained on a website, usually by an individual or by a group of several people.

BLOGOSPHERE

The online community that is made up of all blogs.

CATFISHING

Luring someone into a relationship by a fictional online persona.

CROWDSOURCING

A business term that describes the process of obtaining funding, services, or ideas by soliciting contributions from a group of people, usually online. Numerous people each add a small contribution that combines with others to achieve a result. For example, physicians can solicit ideas and observations about clinical issues through online communities (see Sermo; see Doximity).

DIGITAL FOOTPRINT

The data trail that people leave online. A passive digital footprint describes the information collected without a user's knowing. An active digital footprint describes the information a user knowingly or purposely shares about his or herself through websites and social media.

DOXIMITY

A form of medical crowdsourcing. Doximity is an online social networking service for physicians that offers a searchable directory and HIPAA-secure case collaboration, physician-to-physician messaging, and medical news.

FACEBOOK

A social networking website created by Mark Zuckerberg with his Harvard roommates. Anyone who is at least 13 years old is permitted to become a registered user. Users can create a profile, add "friends," send messages, and share status updates, photos, and videos.

FOURSQUARE

A mobile app that takes in information about the user, such as places he goes, places friends go, and things he has told the app that he likes, and then recommends places to go that are near the user's location that the app determines he might like.

FRIENDING

Adding someone to a list of friends or connections on a social networking website. Friending someone usually gives them some privilege on the website that non-friends do not have, such as making a post or viewing more personal information than the general public is permitted to see.

GOOGLE

(n.) The most used search engine on the Internet where users can search for text on websites, documents, or images among other information.

(v.) The act of running or performing a Google search.

HASHTAG

A label that is used in social networking (i.e. Twitter) or blogging to make it simpler for users to find messages with a specific topic. A hashtag is created by putting the number or pound sign (#) in front of a word or a phrase with no spaces.

HOSTING

An internet service that allows organizations to make their website accessible via the Internet. Host companies provide space on a server that is owned or leased by the client, as well as Internet connectivity.

INSTAGRAM

A social networking service that allows users to take and upload pictures and videos that can be shared on the Instagram app itself and also on platforms such as Twitter, Facebook, and Tumblr. Instagram allows users to add filters to the photos and post them with captions and hashtags.

LIKE

With respect to Facebook and Instagram, to like something means to let a person know you enjoy their status, post, or photograph, etc. without leaving a comment. Usually this is done by clicking a 'like' button.

GLOSSARY (CONT'D)

LINKEDIN

A social networking site that is business-oriented and specifically used for professional networking. Professionals can create a profile that reads much like an online resume, connect with other users, and search for jobs.

LISTSERV

An electronic mailing list. An email sender can send one email to the list, which in turn sends it to all of the email addresses of the subscribers to the list.

METADATA

Data about data, or the basic information about data. For example, a document may contain metadata identifying the author, date created, date modified, and file size. Metadata for webpages contain descriptions of the page's content and the keywords linked to the content, facilitating the generation of results by search engines.

REDDIT

An online bulletin board. Users can post content such as texts and links and then other users can vote submissions up or down to organize the post's position on the webpage. The content on Reddit is organized into subreddits, containing topics such as news, movies, music, and fitness, among others.

SERMO

A form of medical crowdsourcing. Sermo is an online community for physicians where they can post observations and questions about clinical issues and receive other doctors' opinions.

SHARE

To share on social media is to take content, such as an article, picture, or status and repost it on the user's own social media outlet.

SNAPCHAT

A social networking application where users communicate with each other through images, whether that be a photo or a video. These messages are called snaps and can be edited within the app by adding text and drawings. Senders can limit the amount of seconds that snaps are viewable and after this time period the snaps are no longer viewable on the recipient's device but are not deleted from Snapchat's servers.

SOCIAL MEDIA

A general term that describes the online tools that people use to create and share information, ideas, videos, pictures, etc. in virtual communities.

SOCIAL NETWORKING

The act of using an online service or website to facilitate the building of social relations among people who most often share interests, activities, or real-life connections.

TAG

A keyword or term assigned to a piece of information that allows the item to be found again by searching the Internet.

TUMBLR

A blogging platform and social networking site that allows users to post multimedia and other content. Users can follow other members' blogs and can also post (reblog) content from followed blogs.

TWEET

(n.) A message posted on twitter that can contain text, photos, videos, or links. Text cannot exceed 140 characters.

(v.) The act of sending the message.

TWITTER

A microblogging network that allows users to set up profiles and communicate through "tweets," 140-character messages (including photos, videos and links).

YOUTUBE

A video-sharing website where users can upload their own videos and view others' videos.

VIRAL

A video that becomes popular through sharing over the Internet via websites, social media, etc. that often contains humorous content.

WEB 2.0

Emphasizes somewhat of a "second coming" of the Internet where users no longer passively view content but rather generate the content themselves. This content is generated through all types of social media.

WIDGET

A third party application developed for an online social network platform that is meant to make the social network more useful or entertaining to the users.

WIKI

A web application that allows collaborative modification, extension, or deletion of the content and structure. The content has no defined owner or leader. The online encyclopedia project, Wikipedia, is one of the most popular wikis on the Internet.

YELP

A website and mobile app that publishes reviews of restaurants and businesses by users of those establishments. The site also contains information about the business, such as contact information and hours of operation.

SOCIAL MEDIA USE AND MISUSE:

A GUIDE FOR PSYCHIATRISTS





CONTACT

(800) 245-3333

PRMS.com

TheProgram@prms.com

MORE THAN AN
INSURANCE
POLICY