Social Media and Electronic Communications

Introduction

The Washington Medical Commission (WMC) is charged with protecting the public and upholding the standing of the profession in the eyes of the public.[1] The WMC offers this guidance to help practitioners (allopathic physicians and physician assistants) to use social media and electronic communications responsibly and professionally.

Practitioners must adhere to their professional responsibilities at all times, including when using social media and electronic communications. [2] While social media and electronic communication offer many benefits to practitioners and their patients, inappropriate use can harm patients and can result in a loss of trust in the medical profession, patient reluctance to seek medical care, and reputational damage to practitioners and their institutions. [3] This document seeks to guide practitioners on how to minimize the risks inherent in the use of social media and electronic communications to protect their patients, the public, and themselves.

Guidance

Professionalism

1. Ensure all communications, activity, and social media postings are professional, ethical, and do not reflect poorly on the medical profession. Think twice before posting. If you would not comment publicly in your professional or personal capacity, do not do so online.

2. Treat media domains as public, accessible to anyone, regardless of whether it is posted in a closed or private forum and regardless of privacy settings and levels of encryption used. Consider any social media post as permanent, even if it has been deleted.

---

[1] RCW 18.17.003 and *Haley v. Medical Disciplinary Board*, 117 Wn.2d 720 (1991)

[2] Many of the principles in this guidance document were taken from "*Social Media and Electronic Communications*" Federation of State Medical Boards Report and Recommendation of the FSMB Ethics and Professionalism Committee, adopted as policy by the Federation of State Medical Boards April 2019, and "Professional Standards and Guidelines Regarding Physician Use of Social Media" issued by the Physicians & Surgeons of Nova Scotia, approved October 12, 2018, and updated December 10, 2021.

[3] The term "social media" encompasses a wide variety of web and mobile technologies that people use to share content, opinions, insights, experiences, and perspectives online. Social media platforms are constantly changing and include Facebook, Twitter, YouTube, LinkedIn, and discussion forums such as Quora and Reddit. Social media also includes healthcare provider networking sites such as Sermo, Doximity, Daily Rounds, Figure 1, Among Doctors, iMedExchange, and Student Doctor Network.

3. When discussing general medical issues online, identify yourself as a practitioner and provide your name and affiliation. Avoid being anonymous. Any material you post is likely to be viewed as trustworthy and may reasonably be taken to represent the views of the profession more widely.

4. When marketing your practice online, be truthful. Be transparent about any conflicts of interest, financial or otherwise. Do not misrepresent your training, expertise, or credentials.

5. Do not offer a patient an incentive to post a positive review or to remove a negative review from an online customer review site.

6. Communicate and engage in social media in personal and professional settings with civility and respect for others. Do not engage in disruptive behavior such as cyberbullying.[4]

Practitioner-Patient Relationship

7. Maintain appropriate professional boundaries with patients and their surrogates, as well as colleagues, at all times. Do not post anything on social media or in electronic communications that you would not document in a patient's chart or hesitate to explain to patients, their family members, your colleagues, the news media, or the WMC.

8. Do not provide medical advice to specific patients online unless this is done via the secure patient portal of a practice or institution and will become a part of the patient's medical record.

9. Do not conduct internet searches on patients for non-clinical reasons. When considering searching for information about a patient through an online search, ask yourself "Why do I want to conduct this search?" If the reason is simply curiosity or other personal reasons, do not conduct the search.[5]

Consent and Confidentiality

10. Do not post individually identifiable patient information or post images or videos without the express written consent of the patient. The express written consent should include the purposes of the social media posting, where to be posted, who will see the post, and the duration of the post. Note that patient consent does not give you free reign to post images that would be offensive, disrespectful, or distasteful to the general public. Any social media posting involving a patient, or any parts of their body must be respectful, gender and racially sensitive, and meet ethical and moral standards.

11. Do not pressure patients into permitting their images to appear on web sites or social media. Do not offer incentives to patients to permit the use of their images on web sites or social media, or

---

[4] See RCW 9A.46.110.

[5] C. Ventola, *Social Media and Health Care Professionals: Benefits, Risks, and Best Practices,* P&T, Vol 39, no. 7, page 497, July 2014

to post positive reviews or delete negative reviews. Remember that there is a power differential between a practitioner and a patient.

12. Do not obtain informed consent for social media posts at the same time you obtain informed consent for treatment.

13. Do not use the practitioner-patient relationship as a source of entertainment to increase notoriety or attract patients.

14. Maintain patient confidentiality. When publishing content on social media, follow the confidentiality rules for publishing patient information in journals, textbooks, and educational presentations. The consent process required when publishing in a journal and presentation is also required for social media. Never provide any information that could be used to identify a patient, even in a closed or private-online forum. Although individual pieces of information may not breach confidentiality on their own, the sum of published information online could be enough to identify a patient or someone close to them. Privacy settings can be compromised. Content posted on social media is traceable even if posted anonymously.

15. Do not respond to patient reviews—positive or negative—on online review sites without the specific consent of the patient. While a patient may share any information about their experience in an online forum, patient privacy laws still apply. A practitioner may contribute to an online review forum but may not confirm that a person received healthcare services unless the patient signs a written consent specifically permitting the practitioner to reveal information in an online forum. Note that a patient can revoke permission at any time. The Commission recognizes the challenge this presents when a patient may post false or defamatory information; the Commission refers practitioners to resources in the Reference section below for additional guidance.

16. Do not post online customer reviews to a testimonial page on your website or to social media without the specific consent of the patient. Get the patient's written consent before you share or embed their reviews.

17. Social media platforms are available for practitioners to share information and discuss medicine, as well as provide a means for peer-to-peer education and dialogue. Ensure these sites are password protected so that only registered users have access to the information. Assume all social media, including peer-to-peer platforms, to be in the public domain and accessible to all.

Related Laws and WCM Policies and Guidance documents

18. Become familiar with the WMC Guidance Documents on Medical Professionalism, Informed Consent, and Sexual Misconduct.

19. Become familiar with patient confidentiality laws, such as Chapter 70.02 RCW and the HIPAA Privacy Rule[6] and Security Rule[7], as well as relevant copyright, defamation, and harassment laws. You can find an excellent description of how to avoid HIPAA violations using social media in the HIPAA Journal.[8]

Principles and Examples

1. **Principle:** Do not reveal patient information in a post.

   Example: A practitioner posts comments about a patient on Facebook. The practitioner does not mention the patient's name, but there is sufficient information to enable others in the community to identify the patient. Posting any protected health information, even that someone is a patient of yours, onto social media sites may violate privacy laws.

2. **Principle**: Do not use information gained from patient billing, medical records, or conversations with a patient for reasons not permitted by federal and state privacy laws.

   Example: It would be a professional boundary violation to gain knowledge of a patient's home address in medical records or billing systems, and find the house on a map or using an electronic mapping service out of personal curiosity whether or not the practitioner drives to the patient's home.

   Example: It would be inappropriate, and possibly a violation of privacy law, to use information gained from patient records or interviews in order to identify and find a patient on a social media site out of personal curiosity.

   Example: Photos, videos, or comments posted on social media sites may violate privacy laws. It is important also to evaluate carefully if anything in the background of a photo or video may be inappropriate for posting.

3. **Principle:** With few exceptions, do not use social media or electronic communications to inquire into patients' lives for reasons unrelated to clinical care or staff safety. If no clinical or academic research reason exists to make such an inquiry, practitioners should not do so.

   Example: In an emergency department, in order to identify family members of a patient who lacks identification and cannot communicate, it would be acceptable to obtain information from an Internet search.

---

[6] U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html . Accessed June 22,2023.
[7] U.S. Department of Health and Human Services. Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html . Accessed June 22, 2023.
[8] "HIPAA Social Media Rules," *HIPAA Journal*. https://www.hipaajournal.com/hipaa-social-media/#:~:text=Posting%20patient%20information%20on%20social,commit%20fraud%20or%20identity%20theft. Accessed July 6, 2023.

Example: An exception would include when a patient is running for elected office and the practitioner wants to research the patient's political positions in order to determine how to vote.

Example: A physician conducts a Google search to find out more about a patient's job duties. If there is no clinical reason for the search, this is inappropriate.

4. **Principle**: Do not post individually identifiable patient information or post images or videos without the express written consent of the patient.

Example: A patient posts a positive review of a practitioner's care on an online review site. The practitioner posts a short note thanking the patient. This is confirmation that the person received healthcare services from the practitioner. This violates both state and federal law if the patient has not expressly consented.

References

"Social Media and Electronic Communications," Federation of State Medical Boards Report and Recommendation of the FSMB Ethics and Professionalism Committee, adopted as policy by the Federation of State Medical Boards April 2019. https://www.fsmb.org/advocacy/policies/?q=social%20media&s=newest&r=&p=2. Accessed July 6, 2023.

"Professional Standards and Guidelines Regarding Physician Use of Social Media," the College of Physicians & Surgeons of Nova Scotia. Approved October 12, 2018, and updated December 10, 2021. https://cpsns.ns.ca/resource/physician-use-of-social-media/#:~:text=When%20engaging%20in%20social%20media,all%2C%20regardless%20of%20privacy%20settings. Accessed July 6, 2023.

American Medical Association Code of Medical Ethics, Opinion 2.3.2 Professionalism in the Use of Social Media. https://policysearch.ama-assn.org/policyfinder/detail/E-2.3.2%20?uri=%2FAMADoc%2FEthics.xml-E-2.3.2.xml. Accessed July 6, 2023.

C. Ventola, Social Media and Health Care Professionals: Benefits, Risks, and Best Practices, *P&T*, Vol 39, no. 7, page 497, July 2014. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/ accessed July 6, 2023.

B. Nguyen, E. Lu, N Bhuyan, K. Lin, M. Sevilla, "Social Media for Doctors: Taking Professional and Patient Engagement to the Next Level," *FPM*, 2020;27(1):19-24. https://www.aafp.org/pubs/fpm/issues/2020/0100/p19.html. Accessed July 6, 2023.

"When is Posting About Patients on Social Media Unethical "Medutainment," *AMA J Ethics*. 2018;20(4): pages 328–335. doi:10.1001/journalofethics.2018.20.4.ecas1-1804. https://journalofethics.ama-assn.org/article/when-posting-about-patients-social-media-unethical-medutainment/2018-04. Accessed July 6, 2023.

"Medutainment—Are Doctors Using Patient to Gain Social Media Celebrity?" *CMAJ*, May 28, 2018, 190 (21) E662-E663; DPI: https://doi.org/10.1503/cmaj.109-5603. https://www.cmaj.ca/content/190/21/E662. Accessed July 6, 2023.

"Perspectives, Patient-Targeted Googling: The Ethics of Searching Online for Patient Information," *Harv. Rev. Psychiatry*, March/April 2010, pages 103-12. https://psycnet.apa.org/record/2013-22209-024. Accessed July 6, 2023.

"An Expert's Guide to Patient Privacy and Online Reviews," John Carroll, Yelp Official Blog. December 1, 2016. An Expert's Guide to Patient Privacy and Online Reviews | Yelp - Official Blog Accessed June 30, 2023.

"HIPAA Social Media Rules," *HIPAA Journal*. https://www.hipaajournal.com/hipaa-social-media/#:~:text=Posting%20patient%20information%20on%20social,commit%20fraud%20or%20identity%20theft. Accessed July 6, 2023.

Number:	GUI2023-01
Date of Adoption:	July 14, 2023
Revised:	n/a
Supersedes:	GUI2014-02.