SOCIAL MEDIA AND THE MEDICAL PROFESSION

A guide to online professionalism for medical practitioners and medical students

AMA

NEW ZEALAND MEDICAL ASSOCIATION

nzmsa

amsa

A joint initiative of the Australian Medical Association Council of Doctors-in-Training, the New Zealand Medical Association Doctors-in-Training Council, the New Zealand Medical Students' Association and the Australian Medical Students' Association

SOCIAL MEDIA AND THE MEDICAL PROFESSION:

A guide to online professionalism for medical practitioners and medical students

The professional standards of doctors and medical students – which are based on the expectations of the community and medical peers – form the cornerstone of quality patient care. They are taught and assessed from the first year of medical school, and are continually re-emphasised throughout medical training and practice. The Australian and New Zealand Medical Councils have widely accepted guidelines on good medical practice,[1 2] and the Australian and New Zealand Medical Associations (AMA and NZMA) and the Australian Medical Students' Association (AMSA) have developed codes of ethics for their members.[3 4 5]

The world to which these professional standards apply is expanding rapidly. Society has enthusiastically embraced user-generated content such as blogging, personal websites, and online social networking.[6] Research shows that use of social media by the medical profession is common and growing.[7 8] In one 2010 study, 220 out of 338 (65 per cent) medical students at the University of Otago, New Zealand, had a Facebook account.[9]

Although doctors and medical students are increasingly participating in online social media, evidence is emerging from studies, legal cases, and media reports that the use of these media can pose risks for medical professionals. Inappropriate online behaviour can potentially damage personal integrity, doctor-patient and doctor-colleague relationships, and future employment opportunities. Our perceptions and regulations regarding professional behaviour must evolve to encompass these new forms of media.

The Australian Medical Association Council of Doctors-in-Training (AMACDT), the New Zealand Medical Association Doctors-in-Training Council (NZMADITC), the New Zealand Medical Students' Association (NZMSA), and the Australian Medical Students' Association (AMSA) are committed to upholding the principles of medical professionalism. As such, we have created some practical guidelines to assist doctors and medical students to continue to enjoy the online world, while maintaining professional standards.

BE CAREFUL ABOUT WHAT YOU SAY AND HOW YOU SAY IT

Confidentiality:

Example 1:

You are working in a rural hospital and make a comment on a social networking site about an adverse outcome for one of your patients. You are careful not to name the patient or the hospital. However, you mentioned the name of the hospital you are working at in a post last week.

A cousin of the patient searches the internet for the hospital's name in order to find its contact phone number. In the search results, the patient's cousin is presented with your posting mentioning the hospital. The cousin then sees the subsequent posting regarding the adverse outcome involving the patient.

Doctors have an ethical and legal responsibility to maintain their patients' confidentiality. This still applies when using any form of online tool, regardless of whether the communication is with other doctors, a specific group of people (e.g. 'friends' on social networking sites), or the public (e.g. a blog). The anonymity potentially afforded online is no excuse for unprofessional behaviour.

Before putting patient information online, think about why you are doing it. You should inform the patient and gain their express consent, and acknowledge that consent has been obtained in any online posts. If you feel it is appropriate to discuss a patient case – for example, to further that patient's care or the care of future patients who present with a similar condition – care must be taken to ensure that the patient is properly de-identified. Using a pseudonym is not always enough; you might have to change case information or delay the discussion. The accessibility and indexability of online information means that although a single posting on a social networking website may be sufficiently de-identified in its own right, this may be compromised by other postings on the same website, which are just a mouse click away.

In maintaining confidentiality, you must ensure that any patient or situation cannot be identified by the **sum** of information available online.

Breaching confidentiality can result in complaints to your medical registration authority (with potential disciplinary action, including loss of registration), involvement of the Privacy Commissioner, or even legal action (including civil claims for damages). In Australia, Medical Boards have already investigated doctors for patient-identifying information posted on social networking sites.[10 11] Moreover, breaching confidentiality erodes the public's trust in the medical profession, impairing our ability to treat patients effectively.

Defamation:

Example 2:

Dear Emergency Registrar,

Thanks a million for misdiagnosing my patient's perforated bowel as constipation and treating aggressively with laxatives. I'm sure she appreciated the subsequent cardiac arrest and multiorgan failure. Don't worry, she just needs a new set of kidneys and a liver and she'll be right. And with that kind of performance, I'm sure you can help her acquire them.

Kind regards,

Lowly intern

(based on an actual posting on a social networking site)

Another potential risk of inappropriate online comments is defamation.

Defamatory statements:

- Are published to a third person or group of people;
- Identify (or are about) a patient/colleague/person ('subject'); and
- Damage the reputation of the subject.

Professional codes of conduct specify that doctors should not engage in behaviours that can harm the reputation of colleagues or the profession.[12] Be mindful about comments made about colleagues (medical or otherwise), employers, and even health departments. Defamation cases are civil claims, in which substantial monetary compensation can be awarded.

KEEP YOUR FRIENDS CLOSE AND OTHERS … NOT SO CLOSE

Doctor-patient boundaries:

Example 3:

You get a friend request on a social networking site from someone whose name sounds very familiar, but they have a photo of a dog as their profile picture. You accept the request. After looking through their profile page, you realise that it is actually one of your previous patients. The patient sends you a message to let you know that they cannot make their next clinic appointment, but would like to know their histology results from a test ordered while the patient was in hospital. The patient also throws in a cheeky comment about some photos they saw of you wearing swimmers at the beach.

A power imbalance exists between doctors and patients, and the maintenance of clear professional boundaries protects patients from exploitation.[13] Doctors who allow patients to access their entire 'profile' (or similar) introduce them to details about their personal lives well beyond what would normally occur as part of the usual doctor-patient relationship, which may be a violation of professional boundaries. In general, it is wise to avoid online relationships with current or former patients. Boundary violations can occur very easily online, and serious indiscretions may result in disciplinary action against the doctor.

If a patient does request you as a friend on a social networking site, a polite message informing them that it is your policy not to establish online friendships with patients is appropriate. Another mechanism used by some doctors, who often work privately, is to create an online profile that is maintained as their professional page only, or to join a professional social networking site.[14] Patients can become friends or fans of this professional page, which only provides information relevant to the professional practice of that doctor. It is also possible to pay companies to manage social networking profiles.

Other boundaries:

Example 4:

*In September 2008, a Junior Medical Officer in the UK was suspended from work for six weeks after describing a senior colleague as a 'f***ing s***' on an online social networking forum. Another colleague, who happened to be friends with the JMO and the senior colleague, saw the posting and made a complaint about the comments to the JMO's employer. The complainant said she felt compelled to complain after seeing the 'scatological' language used in the posting. The JMO apologised for the comments and organised for their removal from the website.*[15]

Other professional relationships may also become problematic on social networking sites. Think very carefully before allowing others (including employers, other doctors, nurses, allied health professionals, clerks, ancillary staff, students, or tutors) to access personal information.

Colleagues' online conduct:

Inevitably, many people choose to interact with colleagues via social media. While you need to be aware of what they see you doing, you may also notice colleagues posting information online or behaving inappropriately. Looking after colleagues is an integral element of professional conduct, so if you feel that a friend or workmate has posted information online that could be damaging for them, consider letting them know in a discreet way (such as a personal email, text message, or phone call).

CONSIDER THE DESTINY OF YOUR DATA

Extent of access to your information:

Many people are unaware of just how easily accessible and durable their online information is. Even if using the most stringent privacy settings, information on social networking sites may still be widely available, including to various companies and search engines. And deleting information is not sure-fire protection – it is almost certainly still stored somewhere in cyberspace, and theoretically permanently accessible. If there is something that you really do not want some people to know about you, avoid putting it online at all. It is much harder to prevent other people posting information about you online (e.g. photos, videos). However, you can report inappropriate content to site administrators and request that it be removed.

(See www.privacy.gov.au/faq/individuals#social_networking or www.netsafe.org.nz/ for more information).

Employee and college trainee background checks:

Recruiters are increasingly screening potential employees online. Employer surveys have found that between one-fifth and two-thirds of employers conduct internet searches, including of social networking sites, and that some have turned down applicants as a result of their searches.[16 17] In another survey, 21 per cent of colleges and universities said they looked at the social networking of prospective students, usually for those applying for scholarships and other awards and programs. [18]

Be conscious of your online image. While employers and colleges you are applying to may find information about you online that could actually prove to be advantageous (e.g. professional-looking photos, information on your extracurricular activities such as sports or volunteer work), material that portrays you in an unprofessional or controversial light can be detrimental.

Real life examples include an employer who turned down an applicant after discovering that he had used Facebook to criticise previous employers and disclosed company information,[19] a doctor who missed out on a job because the doctor's online activities revealed an interest in witchcraft,[20] and a female psychiatrist who failed to gain employment after a recruiting agency found explicit pictures on MySpace of her intoxicated.[21]

Other issues with employment:

Example 5:

Seven doctors and nurses were suspended from Swindon's Great Western Hospital, UK, after they posted photos of themselves on Facebook playing the 'lying down game' on the hospital premises. The aim of the game is to take photos of yourself lying inert in ridiculous places such as on top of cars, bins, or tables. A hospital manager dobbed in the doctors and nurses after he saw pictures of them on a Facebook site posing on hospital trolleys and ward floors. Hospital management said the staff faced disciplinary action because the hospital set 'high standards for staff behaviour at all times and therefore takes any such breaches extremely seriously'.[22]

Employers and colleges may access online material and activities about their current medical staff or trainees, with potentially career-damaging outcomes. An insurance company employee was fired when she was caught on Facebook after calling in 'sick', having claimed she could not work in front of a bright computer,[23] and a trainee was suspended for making insulting comments about a senior medical colleague on an online forum.[24]

When using social networking sites, think before making offensive comments or jokes, sharing information about unprofessional activities (e.g. involving alcohol or drugs), or joining or creating groups that might be considered derogatory or prejudiced. Although online groups or webrings may seem innocuous, other people will not always treat the group with the same humour.

University regulations:

Medical students are not held to any lesser standards of professionalism than doctors. They may face disciplinary action from their universities and, in Australia where all medical students are registered with the Medical Board of Australia, from the medical registration authority. In New Zealand, although the medical registration authorities do not have jurisdiction over medical students, they do advise disclosure of any infringements of the law or other misconduct as these may affect eventual medical registration.[25]

According to a 2009 US study, 60 per cent of responding deans of medical schools reported that medical students had posted unprofessional content online, including violations of patient confidentiality, use of profanity in reference to specific persons or faculties, discriminatory language, depiction of intoxication, sexually suggestive material, and pictures with illicit substance paraphernalia. In many cases, this led to disciplinary action by the universities, including dismissals.[26]

In other examples, a Twitter comment by an Australian medical student allegedly intended as a joke between friends resulted in an international media storm for referring to US President Barack Obama as a 'monkey'.[27] A student from Ryerson University in Canada was almost expelled for running a Facebook study group where students exchanged thoughts on test questions,[28] while a YouTube video of a medical parody caused a great amount of public upset and embarrassment for the students involved and their American university.[29]

Students are entitled to enjoy an active social life. But remember that online behaviour passed off as 'youthful exuberance' at this early stage in your career will still be available later on, and perhaps be seen in a less favourable light. You also need to consider whether your online activities violate university regulations (check with your university whether it has a policy relating to online behaviour), because this could form the basis of disciplinary action.

TAKE CONTROL OF YOUR PRIVACY

Facebook's privacy settings:

Most social networking sites or blogs will have privacy settings enabling you to control (to some extent) how accessible your material is. The following information regarding Facebook, while specific to that particular site, highlights many of the issues you need to be aware of:

- In 2009, Facebook updated its Privacy Policy and Settings, and automatically defaulted a large number of people back to far more public settings. Facebook changes its privacy settings frequently, so be alert for these sorts of changes in the future. Privacy settings can be accessed by clicking 'Account' in the top right and selecting 'Privacy Settings.' This section also allows you to see what your profile looks like to someone who is not a Facebook friend;
- Your name, profile photo, friends list, gender, geographic location, and pages and networks to which you belong are considered 'publicly available' and do not have privacy settings;
- Even after you remove content from your profile, copies of that information may remain viewable elsewhere if it has been shared with others;
- The default setting for who can access many types of information on Facebook is 'Everyone'. The 'Everyone' setting makes information publicly available to any Facebook user and to search engines for indexing purposes;
- Adding an application to your Facebook profile shares all your profile information with that application and its parent company;
- The Privacy Policy allows for 'Social Advertisement Serving': this means that a Facebook activity you undertake, such as becoming a fan of a page, may be served to one of your Facebook friends, coupled with an advertisement for that page; and
- It is stipulated that Facebook 'cannot ensure that information you share on Facebook will not become publicly available'.

If you want to know more about how secure your information will be when using online forums, make sure you read their privacy policies. If you still have questions or concerns, you can contact the site operator. Additionally, Australia and New Zealand have Privacy Commissioners with expertise in this area (see www.privacy.gov.au or www.privacy.org.nz).

ARE YOU MAINTAINING PROFESSIONAL STANDARDS ONLINE?

Online social media challenge: What is 'public' and 'private'?

Even though medical students and doctors are entitled to a private personal life, online social media have challenged the concepts of 'public' and 'private' and, in turn, changed the way in which online aspects of private lives are accessible to others.[30] Once information is online, it is almost impossible to remove and can quickly spread beyond a person's control. A moment of rashness now could have unintended and irreversible consequences in the future – inappropriate online activities can be detrimental to relationships with patients and colleagues, training and employment prospects, and personal integrity. This is not to say that medical professionals should avoid using social media, because their use can be personally and professionally beneficial. But traditional expectations regarding the conduct of the medical profession still apply in this non-traditional context; medical students and doctors always have a duty to patients and the community to maintain professional standards, including when using online social media.

Troubleshooting: Have you ever ... ?

- Googled yourself? Search for your full name in Google, particularly 'Australian Sites Only' and 'New Zealand Sites Only'. Do you feel comfortable with the results that are shown?
- Posted information about a patient or person from your workplace on Facebook? Have a look through your old online posts and blogs;
- Added patients as friends on Facebook or MySpace?
- Added people from your workplace as friends?
- Made a public comment online that could be considered offensive?
- Become a member or fan of any group that might be considered racist, sexist, or otherwise derogatory? Browse through all the groups that you have joined and consider whether these are an accurate reflection of the person you are, and the values that you hold.
- Put up photos or videos of yourself online that you would not want your patients, employers or people from your workplace to see?
- Checked your privacy settings on Facebook or MySpace?
- Felt that a friend has posted information online that may result in negative consequences for them? Did you let them know?

ACKNOWLEDGEMENT

This guide was developed by representatives from the AMA, NZMA, AMSA, and NZMSA, including Dr Sarah Mansfield, Dr Andrew Perry, Dr Stewart Morrison, Hugh Stephens, Sheng-Hui Wang, Dr Michael Bonning, Rob Olver and Dr Aaron Withers.

Our aim was to develop a simple guide for medical students and doctors that explores various risks posed by online social media. In order to achieve this, a literature review was conducted, which included an exploration of:

- Existing guides to professionalism by representative organisations for the medical profession, registration authorities, and medical defense organisations;
- Medical and non-medical journals in Australasia and abroad;
- Items from media (eg newspaper articles);
- Online discussion forums; and
- Our own interactions with social media.

Where possible, we have also drawn upon real life examples based on our own experiences and those of our colleagues.

We are very grateful to the other members and secretariats of the participating organisations who provided input. In particular, we acknowledge the generous assistance of the AMA with design and administrative support.

REFERENCES

See the references below for additional information. New Zealanders may also find the Medical Council of New Zealand's June 2006 statement on use of internet and email communication helpful:

http://www.mcnz.org.nz/portals/0/Guidance/Use%20of%20the%20internet%20and%20electronic%20communication.pdf

References

1 Australian Medical Council. Good Medical Practice: A Code of Conduct for Doctors in Australia. Canberra: Australian Medical Council, July 2009. http://goodmedicalpractice.org.au/code/ (accessed June 2010).

2 Medical Council of New Zealand. Good Medical Practice: A guide for doctors. Wellington: Medical Council of New Zealand, June 2008 www.mcnz.org.nz/portals/0/guidance/goodmedpractice.pdf (accessed June 2010).

3 Australian Medical Association. AMA Code of Ethics – 2004. Editorially Revised 2006. Canberra: Australian Medical Association, 2006. www.ama.com.au/codeofethics (accessed June 2010).

4 New Zealand Medical Association. NZMA Code of Ethics. Wellington: New Zealand Medical Association, May 2008. http://www.nzma.org.nz/about/ethics.html (accessed June 2010).

5 Australian Medical Students' Association. AMSA Code of Ethics. Canberra: Sept 2003. www.amsa.org.au/docs/ED/AMSA%20Code%20of%20Ethics.pdf (accessed June 2010).

6 Coffield RL, Joiner JE. Risky Business: Treating/Tweeting the Symptoms of Social Media. AHLA Connections [internet]. March 2010 [cited June 2010];14 (3):10-14. http://www.healthlawyers.org/News/Connections/CurrentIssue/Documents/2010%20Connections%20Full%20issues/AC_March2010.pdf

7 Darves, B. Social Media and Physicians. NEJM Career Centre [internet]. March 2010 [cited October 2010]. http://www.nejmjobs.org/career-resources/social-media-and-physicians.aspx

8 Thompson LA, Dawson K, Ferdig R, et al. The intersection of online social networking with medical professionalism. J Gen Intern Med 2008;23:954–7.

9 MacDonald J, Sohn S, Ellis P. (2010) Privacy, professionalism and Facebook: a dilemma for young doctors. Medical Education 44:805-813.

10 Pow, H. Doctors Caught Revealing Secret Patient Information on Facebook Posts. The Sunday Telegraph [internet], September 25 2010 [cited September 2010]. www.news.com.au/technology/doctors-caught-revealing-secret-information-on-facebook/story-e6frfrnr-1225929424789

11 Brill, D. Social Networking: Facing the facts. Medical Observer [internet], May 2010 [cited October 2010]. http://www.medicalobserver.com.au/news/social-networking-facing-the-facts

12 Ibid 3.

13 Ibid.

14 Ibid 11.

15 Graham N, Moore P. The Dangers of Facebook. Stud BMJ 2008;8(10):354-355

16 Parker, K. Web warning for youths: Employers are watching. Washington: Washington Post Writers Group [internet], March 2007. www.realclearpolitics.com/articles/2007/03/peekaboo.html (accessed June 2010).

17 Paton, N. Cyber-vetting managers face backlash. Management Issues [internet]. 18 Oct 2007 [cited June 2010]. http://www.management-issues.com/2007/10/18/research/cyber-vetting-managers-face-backlash.asp

18 Greenwood, B. Facebook: the next great vetting tool? Information Today, Inc. [internet]. 2009; 26(8) (cited June 2010). http://www.infotoday.com/it/sep09/Greenwood.shtml

19 Foster P. Caught on camera – and found on Facebook. The Times [internet]. Jul 17 2007 www.timesonline.co.uk/tol/life_and_style/education/article2087306.ece [accessed June 2010).

20 Dolan LP. Social networking etiquette: Making virtual acquaintances. American Medical News [internet]. Jun 2 2008. www.ama-assn.org/amednews/2008/06/02/bisa0602.htm (accessed June 2010).

21 Du W. Job candidates getting tripped up by Facebook. MSNBC [internet]. Aug 14 2007. www.msnbc.msn.com/id/20202935 (accessed June 2010).

22 Lakeman G. NHS doctors and nurses could be fired for playing Facebook Lying Down Game. Mirror [internet]. Sep 10 2009. http://www.mirror.co.uk/news/top-stories/2009/09/10/a-lying-shame-115875-21661732/ (accessed June 2010).

23 Crowe A. Defriended! Woman fired for surfing Facebook after calling in sick. WalletPop [internet]. Apr 27 2009. www.walletpop.com/blog/2009/04/27/defriended-woman-fired-for-surfing-facebook-after-calling-in-si/ (accessed June 2010).

24 Praitis N. Row after deanery suspends trainee over Doctors.net comments. Pulse [internet]. Aug 11 2008. www.pulsetoday.co.uk/story.asp?storycode=4120357 (accessed 2010).

25 Medical Council of New Zealand. Fitness for registration as a medical practitioner. Wellington: Medical Council of New Zealand. http://www.mcnz.org.nz/Education/Fitnessforregistrationasamedicalpractitioner/tabid/181/Default.aspx (accessed June 2010).

26 Chretien KC. Greysen SR. Chretien JP. Kind T. Online posting of unprofessional content by medical students. JAMA. 2009;302(12):1309-15.

27 Pollard E. Young Lib expelled over Obama monkey slur. ABC News. [internet]. Apr 16 2010. http://www.abc.net.au/news/stories/2010/04/16/2875124.htm?section=justin (accessed June 2010).

28 Brown L. Student faces Facebook consequences. The Star [internet]. Mar 6 2008. www.thestar.com/news/gta/article/309855 (accessed June 2010).

29 Farnan JM, Paro JA, Higa J et al. The YouTube generation: implications for medical professionalism. Perspectives in Biology & Medicine. 2008;51(4):517-24.

30 Boyd, D.M. Taken out of context: American teen sociality in networked publics'. Publics and Publics [internet]. 2008; 1.4.1 Public and Publics), http://www.danah.org/papers/TakenOutOfContext.pdf (accessed July 2010).