Electronic Communications with Patients

Email/Texting:

1. The physician still has an obligation to protect privacy.
2. Only internal portals and email servers are capable of maintaining confidentiality. Public email servers (Gmail, Yahoo, etc) are not considered private. If either the sending or receiving address is outside of a protected system, the information is at risk.
3. In specific circumstances, it may be acceptable to communicate through email/text. Ideally, the physician should try to obtain informed consent prior to sending any information via an unsecure communication channel.
4. If communicating through email/text, only the minimum amount of patient health information should be transmitted. Ideally, very sensitive material should never be sent via an unsecure channel.

Social Media:

1. Social media is considered public. Closed or restricted access groups are not considered private
2. Even with consent, a physician may face criticism if patient information is released via this method.
3. Anything posted on social media can be taken out of context and circulated widely. Physicians are strongly advised to be professional when interacting on social media.
4. Colleges expect physicians to observe appropriate boundaries when dealing with patients. "Friending" or connecting with patients on a personal level through social media may lead to criticism.

Duties and responsibilities

Expectations of physicians in practice

Using electronic communications, protecting privacy

Originally published October 2013; Revised January 2016
P1304-3-E

Technology is changing communication between doctors and patients, and between physicians and other health care providers. While electronic communication can improve patient care and enhance patients' engagement in their care, it can also present unique challenges to patient privacy and confidentiality.

To help members address some of the medical-legal risks with using electronic communications (eCommunications) in their practice, the CMPA has developed an electronic communications consent template [PDF, DOC]. This template, or form, is intended for physicians to use as the basis for an informed discussion with patients about the use of eCommunication tools. It should be modified by physicians to suit the particular circumstances of their practice, and the applicable medical regulatory authority (College) requirements and privacy legislation in their jurisdiction.

The CMPA's experience suggests that, at present, physicians are most interested in using email and instant messaging (texting), videoconferencing (including Skype and FaceTime), patient portals, and various social media applications. All these electronic communication tools can be accessed from a number of devices, including smartphones and tablets.

Physicians are aware of their general obligations to protect patient information. If they are considering using electronic communication tools with patients, they must also be aware of the risks to patient privacy that are inherent in the use of the devices and applications. The risks related to each are not necessarily the same. In addition, while patients need to be informed of the benefits of electronic communications, they must also be informed of the potential risks. Doctors should have an informed consent discussion with patients, and if the tools will be used, patients' consent should be recorded in their records.

The CMPA's electronic communications consent template [PDF, DOC] is offered primarily as a basis for an informed consent discussion, but may also help in developing an appropriate form for documenting consent. It is worth repeating that members should be aware that using the eCommunications consent form is not a substitute for a proper and informed discussion with patients about the risks associated with the use of the technology. It also does not relieve physicians of their obligation to fulfill all applicable jurisdictional privacy obligations.

Communication via email and messaging

Despite their pervasiveness and convenience, email and texting are often the least secure communication tools. Imagine, for a moment, using standard email software to send personal medical information to a patient — and getting the email address wrong. Worse — the email does not bounce back, but rather appears in the mailbox of an unintended recipient. The risks of interception or errors in sending email, texts, or instant messages can be significant. For these reasons, some privacy commissioners have indicated that using unencrypted email and texting with personal health information should be avoided, and in the case of Alberta appropriate security is mandated by the Health Information Act.

Despite any disclaimer physicians may include in the message, they remain responsible for protecting patient health information and preventing unauthorized access. Privacy legislation generally requires that custodians

adopt safeguards to protect the personal health information under their control. Privacy regulators generally agree that the use of encryption software to protect electronic messages is a reasonable safeguard under the circumstances. There are a number of enterprise solutions that can provide encryption, including many patient portals. The protection options that are available outside the institutional environment can be complex and expensive, however more encryption options and applications are becoming available for use on devices such as smartphones.

Physicians considering using unsecured or unencrypted email or messaging should do so only for information that does not include identifiable personal health information.

Patient portals — Active pathways for two-way communication

Patient portals have been used in a limited way in community health practice since the 1990s.[1] In recent years they have evolved into popular, secure interactive tools that can greatly enhance communication between physicians and patients, and help patients better manage their health.

There are multiple communication functions of web-based portals. For example, portals can house patient profiles and medical records, contain patient education documents, generate alerts and reminders for prescriptions and medication management, make the booking of appointments more efficient, and enable quick review of lab reports and follow-up messages to patients.

A growing number of physicians are taking advantage of this technology, particularly in response to patients' demand for accessibility to everyday technologies that increase convenience and access to information. However, physicians using patient portals should clearly understand the benefits and limits of the technology and what steps should be taken to protect personal health information. While some of the functions of portals may appear innocuous, even downloading patient education materials could communicate confidential information about an individual's health status.

Patient portals need to be secure and accessible only by those who are authorized. The chosen platform must have adequate security systems to protect patient information and private online conversations, and to meet the requirements of applicable privacy legislation. Because the technical and security issues with portals can be complex, physicians and institutions should seek appropriate advice.

Patients also need to be informed in advance about how a portal will be used for online communication. They need to be aware that portals should never be used for urgent messages or time-sensitive health issues. Physicians should explain what information is available and what will be shared through the portal. As well, they should also explain that not all information should be shared online and that face-to-face consultations may be required to avoid the possibility that patients may misinterpret results or to ensure appropriate follow-up care.

This discussion with the patient should be noted in the patient record. Consent forms [PDF, DOC] should set out the terms of use for the portal and the patient's consent to its use for those specific purposes. As well, a terms of use agreement [PDF] should be submitted online before the patient is granted a password and access to the portal. These agreements outline the terms and conditions under which patients can use the portal.

Social media

Physicians need to keep privacy and confidentiality in mind when using social media such as Facebook, YouTube, LinkedIn, or Twitter. These networks can be valuable for sharing information for health promotion and for educational purposes. However, physicians should not communicate identifiable patient health information using social media. While some of these networks appear to mimic private one-on-one conversations through a chat function or direct messaging, content communicated via social media is unprotected and publicly accessible.

Despite rigorous use of privacy settings, information shared on social media sites should be considered public forever.

Physicians should review guidelines provided by their College on the use of social media. Some Colleges provide detailed guidelines for sharing information on blogs, discussion forums, and maintaining professionalism.

Remember that social media platforms are public channels and can be considered equivalent to the front page of any newspaper or home page of any website.

Videoconferencing

Videoconferencing is increasingly being used to communicate with and deliver medical services to patients. Platforms such as Skype and FaceTime are frequently employed as telehealth tools, especially to provide clinical care directly to patients who live in remote communities or who have limited access to services outside their home.

The CMPA article, "Videoconferencing consultation: When is it the right choice?", emphasizes the importance of assessing whether videoconferencing is appropriate in the patient's particular circumstances. Physicians should be aware of the limitations of the technology and determine whether it is appropriate to use in each specific circumstance. If the standard of care cannot be met using videoconferencing or patient privacy cannot be adequately protected, then an in-person consultation should be considered. Physicians should also be aware and follow their College's position on the use of videoconferencing.

Reducing risk in eCommunications

Physicians who communicate personal health information electronically need to keep in mind that they are governed by the same legal and professional standards that would apply in other professional settings. For example, physicians should carefully consider how they will document electronic communications in the patient's medical record.

Further, physicians using electronic communication with patients need to be aware of and follow the privacy legislation and College requirements that apply to their practice and jurisdiction.

Physicians should establish policies and procedures for using electronic communications in their practice. Employees should be informed of the risks with each form of electronic communication and trained to follow the policies and procedures.

Finally, physicians should consider what security measures and procedures they will adopt to reduce the risk of privacy breaches. This includes using appropriate protection and privacy settings. A patient's informed consent to eCommunications should be obtained and documented, either through a notation in the patient's medical record or by a signed consent form or terms of use agreement . Even if a consent form [PDF, DOC] or terms of use agreement [PDF] is signed, physicians should still document in the patient's record the discussion with the patient about the risks and limitations of any electronic communication tool(s) that will be used. Physicians need to keep abreast of advances and be informed about privacy and security issues related to their jurisdiction and practice environment.

Additional resources

- *CMPA Good Practices Guide*: eCommunication and Social media
- "Technology unleashed — The evolution of online communication"
- "Social media: The opportunities, the realities"
- "Top 10 tips for using social media in professional practice"

Reference

1. Coach: Canada's Health Informatics Association. Privacy & Security for Patient Portals: 2012 Guidelines for the Protection of Health Information, Special Edition [Internet].Toronto: Coach; 2012 [cited 2016 Jan 15]. 111 p. Available from: http://www.ehealthontario.on.ca/images/uploads/pages/documents/Privacy-Security-for-Patient-Portals.pdf

Safety of care

Improving patient safety and reducing risks

Technology unleashed - The evolution of online communication

Originally published June 2012
P1202-1-E

Electronic health records, email, web portals, social media, smartphones, and tablets. How should physicians weigh the pros and cons of using increasingly popular technologies?

Besides the number of technologies in their practice environment, physicians may also be encountering more patients eager to book medical appointments and check their medical records online. Some may even want to "friend" their physician on Facebook.

When considering whether to use new information technologies, either professionally or personally, physicians should assess the potential benefits and consider the medico-legal risks. When harnessing the potential of the digital age, the key is to know the risk and how to mitigate it.

Information technology is a reality of medical practice and this presents an opportunity to learn how to integrate these new methods into daily practice. The first step is to learn about the platforms, and then reflect on whether and how each might be used in practice.

Understanding the technology, assessing the risk

Electronic medical records

Implementation of electronic medical records (EMRs) in medical practice continues and many practitioners have embraced the possibilities of improved care through the use of EMRs.

The 2010 National Physicians Survey found that 39% of practising physicians now use EMRs[1]. With 82% of second-year residents reporting that they intend to use EMRs, the use of EMRs is expected to continue rising.

The EMR is a foundational electronic platform that facilitates access to medical records on various digital devices. While most family physicians access records in their office, specialists are more likely to access EMRs from hospitals or health centres. Many physicians surveyed can access the records from home, and close to half of the youngest physicians surveyed access records from a laptop.

Electronic medical records are poised to be accessed increasingly from mobile devices. Using a system which is certified in the physician's jurisdiction is key to the security of patient files and to help meet the legal obligations of privacy and confidentiality. The CMPA has written extensively on the use and implementation of EMRs ("Electronic Records Handbook"), as well as on privacy and confidentiality. These resources are available on the CMPA website.

Email

While email technology is almost two decades old, the medical community has been cautious in adopting it to interact with patients.

According to the 2010 National Physicians Survey, only 16% of physicians use email with patients for clinical purposes. Meanwhile, 58% use email to contact professional colleagues.

There are several potential risk areas in email communication including privacy and security, timeliness of responses, and clarity of communication. Before engaging in email communication, members should review any applicable statutory or regulatory authority (College) requirements that may impact the use of email for transmitting patient health information. Consent by the patient to this form of communications is also important. As well, all emails and attachments should have adequate encryption.

The CMPA has written extensively on the medico-legal risks of using email for professional purposes. For additional information on how best to mitigate the risk of using email, including patient consent forms, see "Consent to use electronic communications [PDF, DOC]".

Web portals

The full potential of web portals has yet to be harnessed, but the promise of timely communication with patients is enticing.

Several specialized websites provide private online environments designed for physician interaction with patients. One of the longest standing web portals, mydoctor.ca, was created in 2008 by the Canadian Medical Association. It is only one of several "health portals."[2]

These portals allow physicians to share medical information with patients, prescribe directly to patients, provide information on a physician's schedule, allow patients to book appointments, provide alerts to patients regarding follow-up care, and allow patients to view their medical history and test results. Most sites also provide secure messaging between the physician and patient, and some provide online networking environments where patients can share information with other patients.

Information stored on portals can be accessed from desktop computers as well as mobile devices, allowing patients and their physicians to monitor health indicators such as blood pressure or blood-glucose levels.

Like all uses of technology, physicians must weigh the potential benefits and the medico-legal risks. While providing patients with information online may empower patients and encourage them to become active participants in their own healthcare, some patients may misinterpret results and jump to conclusions. And, as with all online correspondence, lack of clarity and miscommunication can add complexity to doctor-patient relationships.

Physicians who want to make their services available through a web portal should ensure the chosen platform has adequate security systems to protect patient information and that the requirements of the applicable privacy legislation are respected. Patients should be made aware that portals should never be used for urgent or time-sensitive health issues. Informed consent is key and the physician should keep a record of the patient's agreement to this use of technology.

Mobile devices

In some hospitals, physicians are putting away the standard clipboard and pencil, and are instead opting for the use of tablets.

These tablets — essentially small computers — provide access to email and the Internet, and allow the viewing of learning videos or podcasts. Tablets can interface with other computers wirelessly and can provide access to medical facts, drug-related information, medical calculators, as well as word processors and spreadsheet software. These devices can make the interface with EMRs almost seamless.

Similarly, smartphones are creating an opportunity for doctors and other healthcare professionals to access information wherever they may be — whether working shift in a hospital, or seeing patients in daily office practice.

Some physicians are using mobile devices for remote monitoring of patient care, bridging the distance between physician and patient — a kind of long-distance house call. For example, a physician who is out-of-town may check on patients with chronic conditions such as diabetes or high blood pressure, or visually verify post-operative incisions.

There are a number of precautions that physicians need to consider to avoid medico-legal difficulties. If accessing EMRs from a mobile device, for example, the physician should verify that patient information is encrypted and security levels are adequate to meet the privacy requirements of the jurisdiction. Devices should be password protected, and it may be possible to remotely lock or "wipe" all information from the device should it be stolen or lost. Such measures help ensure that the content stored on the device is not viewed by unauthorized users, even inadvertently.

Social media

Canadian physicians are becoming increasingly aware of the potential of social media — particularly for learning and sharing knowledge — and some medical organizations and societies now use social media tools.

The 2010 National Physicians Survey reports that more than 51% of physicians were using Facebook for personal reasons, while 20% were using other platforms such as Twitter and LinkedIn. The same survey notes that 22% of physicians used online discussion forums with other physicians for professional purposes.

However, online networking is raising issues related to professionalism and ethics, and even personal use of social media by physicians can prompt questions concerning privacy and confidentiality.

Whether a physician has found an audience on a micro-blogging site such as Twitter, posts videos on YouTube, connects with colleagues through LinkedIn, or blogs about health-related issues, keeping patient information confidential and secure is paramount.

The line between professional and personal is often blurry for physicians. Some Colleges have issued guidelines about the use of social media and physicians should check regularly for new policies and updates. Physicians should consider the following:

- Social media platforms should be treated as virtual public spaces, used by millions and potentially accessible by anyone.[3]
- Physicians who communicate through social media, on web portals, or via email should be mindful that they are governed by the same professional and ethical standards as would apply in a physical environment (e.g. hospital setting, family practice).

- The laws on defamation, copyright, and plagiarism apply equally to the web and social media as to print and verbal communication.
- Privacy legislation and licensure require that physicians guard against disclosing any information that could identify a patient. These requirements apply no matter the technology or electronic platform.
- Physicians considering the use of social media should review the policies or guidelines of their College. The Canadian Medical Association has also published guidelines entitled *Social media and Canadian physicians – Issues and rules of engagement*.
- Physicians who use social media are advised to activate the strictest privacy settings whenever possible. On Facebook or LinkedIn, for example, users can adjust privacy settings within the profile sections of their pages. Remember, however, that even though privacy settings have been adjusted, confidential information should not be shared on public social sites.

The field of technology evolves rapidly, often prompting questions regarding risks and benefits. When in doubt about the use of new technologies and of social media, members should not hesitate to call the CMPA for advice or guidance.

References

1. 2010 National Physician Survey. Retrieved on February 2012 from: http://www.nationalphysiciansurvey.ca/nps/home-e.asp
2. mydoctor.ca is hosted by the Canadian Medical Association. There are also several privately owned web portals including mypatientaccess.ca, HealthConnex, myOSCAR, etc.
3. The College of Physicians and Surgeons of British Columbia, "Social media and Online Networking Forums," September 2010.

Safety of care

Improving patient safety and reducing risks

Social media: The opportunities, the realities

Originally published October 2014
P1404-1-E

Virtual interactions and exchanges have never been more frequent. Individuals in most parts of the world can now exchange information instantaneously, to one person or a million. The ability to learn and share is vast — largely driven by social media.

For the medical professional, social media offer opportunities and innovative options for sharing information. Along with the innovation, however, comes risks such as online content that is inaccurate, is unmoderated, attributed to the wrong author, violates privacy, blurs professional and personal activities, and hurts reputations.

Physicians should recognize the impact of social media, and consider how much they want to engage and how to mitigate any potential risks.

Learning and sharing

Medical trainees and faculties are increasingly leveraging several social media sites to enrich trainees' medical education. Students are looking for opportunities to exchange and learn beyond the formal education setting, often using mobile devices to capture and share clinical learnings on social media sites. Facebook, Twitter, LinkedIn, YouTube, SlideShare, Flickr, and blogs are among the most popular sites.[1]

Students and faculty have an obligation to protect the privacy of patients and must refrain from sharing identifiable patient cases through social media, unless the patient has consented. This principle applies regardless of whether the platform's privacy setting is public or private. Some medical regulatory authorities (Colleges) remind physicians that confidentiality may be breached if patients, while not expressly named, can still be identified in an online case example.[2]

It is recognized that generic case examples or other learning material that does not contain identifiable patient information can help students learn. As physicians strive to keep current and abreast of medical findings, social media can prove invaluable.[3]

Patient engagement with social media

Patients are also participating in social media to keep current on health matters.[4] Some join online patient groups to exchange information with others experiencing similar health conditions. Hungry for information, treatment options, and hope, patients may be acquiring knowledge that is inaccurate or inappropriate for their medical condition. However, it is comforting to know patients continue to view physicians as the most valuable source of information for their medical condition.[5]

As patients seek to share their clinical experience with others, they may wish to capture the physician-patient encounter or procedure for social media sharing. Physicians will want to consider how to manage these situations, recognizing the broad reach of social media and the beneficial impact this may have. Physicians who decline to participate should explain why so the patient understands the decision.

Most hospitals and facilities have policies governing the use of photographs or videos during doctor-patient exchanges. If in private practice, physicians may wish to develop policies or guidelines to help manage such requests.

Professional social media engagement

Physicians have long recognized and applied professional behaviour in all facets of care and private life. This behaviour extends to social media, where society's expectations of doctors remain the same as in "real life."

The consequences of unprofessional behaviour over social media are often more significant because of its reach and permanency. Once posted or recorded, the ability to retract a comment is very limited.

At times, social media content gives a false sense of detachment. Because of this, users may post responses or interact in ways that would be considered inappropriate in face-to-face encounters. Doctors should always ask themselves:

- Is this how I would frame my response, if the individual or group was in my office, or if I was in direct contact?
- Is my response typical of how I interact?
- Will I feel the same way tomorrow, or 2 months from now, or 1 year from now, when my comment or contribution remains publicly available?
- Will my response respect my professional obligations?

Know the obligations

Physicians have a duty to protect the personal health information of their patients, including on social media. Both physicians and patients should be aware of the risks and agree to certain conditions before engaging in electronic communications.

False or incorrect information can spread quickly and broadly through social media. This introduces a risk for both patients and their doctors. Imagine having a discussion with a patient about a recommended treatment which has been portrayed as dangerous on social media. Patients may be conflicted and may decline the treatment, based on false information.

Physicians are well-positioned to correct misinformation with patients. While physicians don't have an obligation to monitor everything that is stated on social media, they may want to contribute to the exchange with a view of providing factual information that will benefit others. When it comes to a physician's own social media platform, it is important to monitor what is said and be prepared to correct or interject when necessary.

Leverage social media

The value of social media in public health is well recognized. It broadens the opportunity to alert a community of outbreaks, vaccination centres, and measures that can be taken to mitigate exposure to contagious diseases.

Choosing the appropriate social media site is important. Weblogs, instant messaging platforms, video chat, and social networks can all be valuable platforms with benefits such as:

- reaching large numbers of professionals for public health and policy exchanges
- connecting with professionals at the national and international level to advance research, treatment, and care options
- disseminating timely health information to trigger action

Physicians who use blogs or other social media sites to discuss health-related issues may want to include a reference to the Canadian context in which the information is provided. This will help mitigate the risks of non-Canadians heeding advice that may not be appropriate or relevant.

Publishing information on blogs or other social media platforms could result in legal actions being brought outside of Canada. The CMPA will not generally provide assistance to members who encounter medico-legal difficulty arising from the publication of information to a non-medical audience, when the matter is brought outside of Canada.

Consider the level of engagement

Whether doctors choose to engage in social media or not, they cannot ignore the implications.

If you are not active on social media, you should consider:

- Learning enough about it to understand the implications for your patients, colleagues, and other members of the healthcare team.
- Making an assessment of the potential benefits and risks, and being prepared to explain your decision to not participate to patients, colleagues, and others.
- Recognizing that even if you're not participating, what you say or do can still be shared online.
- Developing a social media policy for your practice and sharing it with your staff and patients. Stating that you're not engaging may help manage the expectations of staff and patients.
- Determining if it is worthwhile to monitor what is said online about you and your practice.

Engaging on social media — on a personal basis

- Recognize that delineating your personal and professional life on social media is often difficult, but you will want to separate the two as much as possible.
- Act on social media as you would in your personal and professional life (virtual behaviour should mirror real-life behaviour).[6] Compassion, respect, and integrity also belong on social media.
- Do not "friend" patients on social media sites, as it becomes difficult to separate professional activities from personal ones. Just as with in-person consultations, remember that professional boundaries also apply to social media.
- Recognize that irrespective of privacy settings, most of what is shared on social media is accessible broadly.
- Appreciate the implications of what you share, albeit personal, to your professional life, as the two are often blurred.
- Recognize the permanency of what is shared on social media and the difficulty in retracting or removing content.
- Monitor what is said on social media about you and be prepared to correct or interject when and if appropriate.
- Review and comply with your College guidance on the use of social media.

Engaging on social media — on a professional basis

- Assess and determine which social media sites align with your objectives (e.g. blogs for sharing healthy lifestyle tips; Twitter to provide timely updates; Facebook to network; YouTube to post educational videos).
- Establish guidelines on the use of social media, including the expectations for your staff. Make your guidelines known to patients, colleagues, and other healthcare providers.
- Determine if you are the only contributor or if others will support your social media activities. Establish protocols for passwords and renew them often, to avoid misappropriation of your social media identity.
- Recognize that your activities on social media are an extension of your professional activities.
- Establish measures to ensure that patients' personal health information remains private and confidential, unless patients have provided consent.

- Maintain appropriate professional boundaries and ensure that medical information posted is not seen as establishing a therapeutic relationship with online users.[7] Information should remain general and geared to broad-based issues (e.g. vaccination).
- Media are often leveraging social media to identify opinion leaders or experts on specific topics — determining ahead of time your interest, preparedness, and availability for media interviews will be helpful.
- Recognize the permanency of what is shared on social media and the difficulty in retracting or removing content.
- Monitor what is said on your social media site and be prepared to correct or interject when and if appropriate.
- Review and comply with your College's policies or guidelines on the use of social media.

The value remains

Social media can be a powerful platform to improve healthcare decisions, share knowledge, and promote adherence to healthy lifestyles. When managed effectively, it can contribute to beneficial exchanges of information. Its full potential has yet to be realized and despite its well-recognized pitfalls, the value of social media remains.

Suggestions to help you get started on social media[8]:

1. Learn about the various sites and determine which one will help you reach your intended audience. Different platforms serve different purposes. Set social media objectives for yourself and select the appropriate platform(s) to achieve them.
2. Become familiar with the security settings and policies. Before benefiting from the information you'll find on social media, educate yourself on the security settings for each platform and the social media policies that pertain to your organization.
3. Join, listen, learn. Before engaging, create a profile on Twitter and Facebook, for instance, and observe the conversations.
4. Learn to manage your social media time. The amount of information shared on social media can be overwhelming. Learn how to filter what is relevant to you to make it more manageable.

References

1. Pearson Learning Solutions. "Teaching, Learning, and Sharing: How Today's Higher Education Faculty Use Social Media," 2011. Accessed on May 24, 2014 from: http://files.eric.ed.gov/fulltext/ED535130.pdf
2. College of Physicians and Surgeons of British Columbia, Professional Standards and Guidelines, Social Media and Online Networking Forums, September 2010. Accessed on June 5, 2014 from: https://www.cpsbc.ca/files/pdf/PSG-Social-Media-and-Online-Networking-Forums.pdf
3. Bahner, David, Adkins, Eric, Patel, Nilesh, Donley, Chad, Nagel, Rolllin, Kman, Nicholas, "How we use social media to supplement novel curriculum in medical education," Medical Teacher, (2012) Vol. 34 No.6. Accessed on May 23, 2014, from: http://informahealthcare.com/doi/abs/10.3109/0142159X.2012.668245
4. Chen, Xueyu, Siu, Lillian, "Impact of the Media and Internet on Oncology: Survey of Cancer Patients and Oncologists in Canada," Journal of Clinical Oncology, (December 1, 2001) Vol. 19 No.23. Accessed on May 23, 2014 from: http://jco.ascopubs.org/content/19/23/4291.short
5. Ibid, Accessed on May 23, 2014 from: http://jco.ascopubs.org/content/19/23/4291.short
6. Canadian Medical Association, "Social media and Canadian physicians – issues and rules of engagement." Accessed on May 23, 2014 from: http://www.cma.ca/advocacy/social-media-canadian-physicians

7. College of Physicians and Surgeons of British Columbia, Professional Standards and Guidelines, Social Media and Online Networking Forums, September 2010. Accessed on June 5, 2014 from: https://www.cpsbc.ca/files/pdf/PSG-Social-Media-and-Online-Networking-Forums.pdf
8. Royal College of Physicians and Surgeons of Canada. "Is your practice social media savvy? Four tips to get you started!," Dialogue, (January 2014) Vol. 14, No.1. Accessed on April 30, 2014 from: http://www.royalcollege.ca/portal/page/portal/rc/resources/publications/dialogue/vol14_1/social_media

Safety of care

Improving patient safety and reducing risks

Top 10 tips for using social media in professional practice

Originally published October 2014
P1404-3-E

1. Have an objective and select the right platform

Physicians should have clear objectives for their professional social media presence so they can select the most appropriate social media site. If your goal is engagement, then platforms such as Facebook and Twitter may be appropriate. If the aim is teaching and learning, then private physician networks may be the best choice. To disseminate health information to benefit the public, blogs may be considered. If the goal is advocacy or a call to action, media interviews with potential social media exposure may generate the desired outcome.

2. Avoid social media for one-on-one discussions

Doctors must remember that social media can be used to engage in public communication, but it is not appropriate for private conversations. Social media may be ideal to connect with patients collectively on issues such as general health promotion or office administration, but you must not communicate specific patient health information to an individual over social media. While some sites appear to facilitate private conversations through direct messages, content communicated via social media is unprotected and publicly accessible. Confidentiality of patient information can be placed at risk.

3. Establish clear boundaries

Whatever platform you use, you need to keep clear boundaries between your professional and personal social media use. For example, if using Facebook both professionally and personally, it's best to have a separate account for each. And, the high standard of behaviour that physicians are held to (by statute and professional necessity) also extends to your social media use.

4. Recognize that the reach is wide and the audience unknown

Because social media has a broad reach, it can be difficult for physicians to know their audience and tailor their messages. As a result, your information should be general in nature and directed at a non-scientific audience. With no physical barriers to the Internet, the information may be used by Canadians or people in other countries.

5. Consider the impact of your communication style and reach

Communication principles that apply when speaking to patients, stakeholders, or the media also apply when using social media. You should use clear language, have supporting examples that respect privacy and confidentiality when giving an opinion, provide credible sources and research, address all sides of an issue, and present information professionally. Remember that information shared via social media can have a significant and lasting impact. When contributing to social media, keep in mind that the information reaches far and wide, and is permanent.

6. Generate interest, participation

The very nature of social media is to invite people to review, share, respond, and contribute to information. Comments, reactions, support, and contrary views are all part of the landscape and should be delivered respectfully. Each participant brings their unique perspective to the discussion. In other words, social media is a two-way street and you should be prepared to be part of a dialogue, when appropriate.

7. Be aware that libel, slander, and defamation apply

Defamation — that is making false statements that can harm the reputation of an individual or an organization — carries the same consequences whether it appears online or in traditional media. When defamatory statements are published or spoken online or otherwise, you may face allegations of libel or slander. As well, you should be aware of the potential for cyber libel — when something posted on the Internet is both untrue and damaging.

You must also realize that plagiarism and copyright infringement can lead to legal action.

8. Develop a social media policy

Physicians should determine how they will use social media — to engage patients or disseminate information, or both. When it's appropriate, physicians may choose to answer certain questions or respond to comments in a discussion, however they should be mindful of the content and the audience.

When you state in a policy or guideline how you intend to use social media, it sends a clear message to patients and others on what to expect. Guidelines should be communicated and apply to staff, patients, colleagues, and other healthcare providers working within your office.

9. Manage privacy and minimize breaches

Some social media platforms allow physician-only groups to participate and share expertise in a way that mimics grand rounds in hospitals where doctors gather to discuss cases. Physicians must recognize these online practitioner communities are still virtual spaces and can be subject to security breaches.

When using social media, you must always consider what security measures and procedures should be adopted to reduce privacy breaches. This includes using appropriate protection and privacy settings to avoid communicating patient health information.

10. Follow College guidelines

Medical regulatory authorities (Colleges) recognize that physicians are using social media in their practice and have created material to guide physicians on how to engage online while meeting legal and professional obligations. The material includes information on how to respect professional boundaries and the importance of exercising caution when posting information that could identify a patient.

CONSENT TO USE ELECTRONIC COMMUNICATIONS

This template is intended as a *basis for an informed discussion*. If used, physicians should adapt it to meet the particular circumstances in which electronic communications are expected to be used with a patient. Consideration of jurisdictional legislation and regulation is strongly encouraged.

PHYSICIAN INFORMATION:

Name:

Address:

Email (if applicable):

Phone (as required for Service(s)):

Website (if applicable):

The Physician has offered to communicate using the following means of electronic communication ("the Services") [check all that apply]:

☐ Email	☐ Videoconferencing (including Skype®, FaceTime®)
☐ Text messaging (including instant messaging)	☐ Website/Portal
☐ Social media (specify):	
☐ Other (specify):	

PATIENT ACKNOWLEDGMENT AND AGREEMENT:

I acknowledge that I have read and fully understand the risks, limitations, conditions of use, and instructions for use of the selected electronic communication Services more fully described in the Appendix to this consent form. I understand and accept the risks outlined in the Appendix to this consent form, associated with the use of the Services in communications with the Physician and the Physician's staff. I consent to the conditions and will follow the instructions outlined in the Appendix, as well as any other conditions that the Physician may impose on communications with patients using the Services.

I acknowledge and understand that despite recommendations that encryption software be used as a security mechanism for electronic communications, it is possible that communications with the Physician or the Physician's staff using the Services may not be encrypted. Despite this, I agree to communicate with the Physician or the Physician's staff using these Services with a full understanding of the risk.

I acknowledge that either I or the Physician may, at any time, withdraw the option of communicating electronically through the Services upon providing written notice. Any questions I had have been answered.

Patient name:

Patient address:

Patient home phone:

Patient mobile phone:

Patient email (if applicable):

Other account information required to communicate via the Services (if applicable):

Patient signature:	Date:
Witness signature:	Date:

APPENDIX

Risks of using electronic communication

The Physician will use reasonable means to protect the security and confidentiality of information sent and received using the Services ("Services" is defined in the attached Consent to use electronic communications). However, because of the risks outlined below, the Physician cannot guarantee the security and confidentiality of electronic communications:

- Use of electronic communications to discuss sensitive information can increase the risk of such information being disclosed to third parties.
- Despite reasonable efforts to protect the privacy and security of electronic communication, it is not possible to completely secure the information.
- Employers and online services may have a legal right to inspect and keep electronic communications that pass through their system.
- Electronic communications can introduce malware into a computer system, and potentially damage or disrupt the computer, networks, and security settings.
- Electronic communications can be forwarded, intercepted, circulated, stored, or even changed without the knowledge or permission of the Physician or the patient.
- Even after the sender and recipient have deleted copies of electronic communications, back-up copies may exist on a computer system.
- Electronic communications may be disclosed in accordance with a duty to report or a court order.
- Videoconferencing using services such as Skype or FaceTime may be more open to interception than other forms of videoconferencing.

If the email or text is used as an e-communication tool, the following are additional risks:

- Email, text messages, and instant messages can more easily be misdirected, resulting in increased risk of being received by unintended and unknown recipients.
- Email, text messages, and instant messages can be easier to falsify than handwritten or signed hard copies. It is not feasible to verify the true identity of the sender, or to ensure that only the recipient can read the message once it has been sent.

Conditions of using the Services

- While the Physician will attempt to review and respond in a timely fashion to your electronic communication, **the Physician cannot guarantee that all electronic communications will be reviewed and responded to within any specific period of time. The Services will not be used for medical emergencies or other time-sensitive matters.**
- If your electronic communication requires or invites a response from the Physician and you have not received a response within a reasonable time period, it is your responsibility to follow up to determine whether the intended recipient received the electronic communication and when the recipient will respond.
- Electronic communication is not an appropriate substitute for in-person or over-the-telephone communication or clinical examinations, where appropriate, or for attending the Emergency Department when needed. You are responsible for following up on the Physician's electronic communication and for scheduling appointments where warranted.
- Electronic communications concerning diagnosis or treatment may be printed or transcribed in full and made part of your medical record. Other individuals authorized to access the medical record, such as staff and billing personnel, may have access to those communications.
- The Physician may forward electronic communications to staff and those involved in the delivery and administration of your care. The Physician might use one or more of the Services to communicate with those involved in your care. The Physician will not forward electronic communications to third parties, including family members, without your prior written consent, except as authorized or required by law.
- You and the Physician will not use the Services to communicate sensitive medical information about matters specified below [check all that apply]:
  - ☐ Sexually transmitted disease
  - ☐ AIDS/HIV
  - ☐ Mental health
  - ☐ Developmental disability
  - ☐ Substance abuse
  - ☐ Other (specify):
- You agree to inform the Physician of any types of information you do not want sent via the Services, in addition to those set out above. You can add to or modify the above list at any time by notifying the Physician in writing.
- Some Services might not be used for therapeutic purposes or to communicate clinical information. Where applicable, the use of these Services will be limited to education, information, and administrative purposes.
- The Physician is not responsible for information loss due to technical failures associated with your software or internet service provider.

APPENDIX CONTINUED

Instructions for communication using the Services
To communicate using the Services, you must:

- Reasonably limit or avoid using an employer's or other third party's computer.
- Inform the Physician of any changes in the patient's email address, mobile phone number, or other account information necessary to communicate via the Services.

If the Services include email, instant messaging and/or text messaging, the following applies:

- Include in the message's subject line an appropriate description of the nature of the communication (e.g. "prescription renewal"), and your full name in the body of the message.
- Review all electronic communications to ensure they are clear and that all relevant information is provided before sending to the physician.
- Ensure the Physician is aware when you receive an electronic communication from the Physician, such as by a reply message or allowing "read receipts" to be sent.
- Take precautions to preserve the confidentiality of electronic communications, such as using screen savers and safeguarding computer passwords.
- Withdraw consent only by email or written communication to the Physician.
- **If you require immediate assistance, or if your condition appears serious or rapidly worsens, you should not rely on the Services.** Rather, you should call the Physician's office or take other measures as appropriate, such as going to the nearest Emergency Department or urgent care clinic.
- Other conditions of use in addition to those set out above: *(patient to initial)*

I have reviewed and understand all of the risks, conditions, and instructions described in this Appendix.

Patient signature

Date

Patient initials_____

CONSENTEMENT À L'UTILISATION D'UN MOYEN DE COMMUNICATION ÉLECTRONIQUE :

Ce formulaire type est destiné à servir *de base pour une discussion visant à obtenir un consentement éclairé.* Les médecins qui l'utilisent devraient l'adapter aux situations particulières dans lesquelles des communications électroniques avec un patient seront susceptibles d'être utilisées. Il est vivement recommandé de tenir compte des lois et règlements de la province ou du territoire concerné.

RENSEIGNEMENTS SUR LE MÉDECIN :

Nom :

Adresse :

Courriel (le cas échéant) :

Téléphone (nécessaire pour le ou les Services) :

Site web (le cas échéant) :

Le médecin offre la possibilité de communiquer avec lui à l'aide des moyens de communication électronique (ci-après « les Services ») [cocher toutes les cases qui s'appliquent] :

☐ Courriel	☐ Vidéoconférence (y compris Skype[MC], FaceTime[MD])
☐ Messagerie texte (y compris messagerie instantanée)	☐ Site web/portail

☐ Réseaux sociaux (préciser) :

☐ Autre (préciser) :

ATTESTATION ET CONSENTEMENT DU PATIENT :

J'atteste, par la présente, avoir lu et pleinement compris les risques, restrictions, conditions et consignes d'utilisation des services de communication électronique choisis et dont une description complète se trouve en annexe de ce formulaire de consentement. Je comprends et accepte les risques énumérés dans l'annexe de ce formulaire qui sont associés à l'utilisation des Services dans le cadre de communications avec le médecin ou les membres de son personnel. Je consens aux conditions et me conformerai aux consignes énumérées dans l'annexe, ainsi qu'à toute autre mesure que le médecin pourrait imposer relativement à la communication avec des patients utilisant les Services.

Je reconnais et je comprends qu'en dépit de l'utilisation recommandée d'un logiciel de chiffrement comme système pour sécuriser les communications électroniques, il est possible que les communications avec le médecin ou les membres de son personnel utilisant les Services, ne soient pas chiffrées. Je consens, néanmoins, en pleine connaissance des risques, à communiquer avec le médecin et les membres de son personnel au moyen de ces Services.

Je reconnais que le médecin, ou moi-même, pouvons en tout temps, sur préavis écrit, mettre fin à l'option de communiquer au moyen des Services. Je reconnais par ailleurs avoir obtenu réponse à toutes mes questions.

Nom du patient :

Adresse du patient :

Téléphone au domicile du patient :

Téléphone cellulaire du patient :

Courriel du patient (le cas échéant) :

Autres renseignements requis pour communiquer au moyen des Services (le cas échéant) :

Signature du patient :	Date :
Signature du témoin :	Date :

Risques associés à l'utilisation d'un moyen de communication électronique

Le médecin utilisera des moyens raisonnables en vue de protéger la sécurité et la confidentialité des informations envoyées et reçues au moyen des Services (le terme « Services » est défini dans le formulaire de consentement à l'utilisation d'un moyen de communication électronique ci-joint). Cependant, en raison des risques mentionnés ci-dessous, le médecin ne peut garantir la sécurité et la confidentialité des communications électroniques :

- Le recours aux communications électroniques pour discuter de renseignements délicats peut accroître le risque que de tels renseignements soient divulgués à des tiers.
- En dépit d'efforts raisonnables pour protéger les renseignements personnels et assurer la sécurité des communications électroniques, il n'est pas possible de sécuriser totalement ces renseignements.
- Les employeurs et les services en ligne peuvent avoir un droit reconnu par la loi d'inspecter et de conserver les communications électroniques reçues et transmises par leur système.
- Les communications électroniques peuvent introduire un logiciel malveillant dans un système informatique risquant ainsi d'endommager l'ordinateur, le réseau informatique ou les systèmes de sécurité, ou d'en perturber le fonctionnement.
- Les communications électroniques peuvent être réacheminées, interceptées, diffusées, mises en mémoire ou même modifiées sans que le médecin ou le patient ne le sache ou ne l'ait autorisé.
- Même si l'expéditeur et le destinataire ont supprimé les messages électroniques, il peut y avoir des copies de sauvegarde sur un système informatique.
- Les communications électroniques peuvent être divulguées en vertu d'une obligation de signalement ou d'une ordonnance du tribunal.
- Les services de visioconférence offerts par Skype[MC] ou FaceTime[MD] peuvent être plus vulnérables aux interceptions que d'autres systèmes de visioconférence.

L'utilisation de courriels ou de messages texte comme moyen de communication électronique comporte les risques supplémentaires suivants :

- Les courriels, les messages texte et les messages instantanés peuvent être facilement réacheminés, ce qui augmente le risque d'envoi non intentionnel à un destinataire inconnu.
- Il est plus facile de falsifier un courriel, un message texte ou un message instantané qu'un document écrit à la main ou signé.
- Par ailleurs, il est impossible de vérifier l'identité de l'expéditeur ou de s'assurer que seul le destinataire pourra lire le courriel une fois qu'il est envoyé.

Conditions d'utilisation des Services

- Bien que le médecin s'efforce de lire et de répondre promptement aux communications électroniques, **il ne peut pas garantir qu'il les lira ou y répondra dans un délai précis**. Par conséquent, **les Services ne doivent pas être utilisés dans les cas d'urgence médicale ou d'autres situations devant être traitées rapidement**.
- Si une communication électronique nécessite ou demande la réponse du médecin et qu'aucune réponse n'est reçue dans un délai raisonnable, il incombe au patient de faire un suivi afin de déterminer si le destinataire visé a bien reçu la communication, et à quel moment celui-ci y répondra.
- Les communications électroniques ne peuvent se substituer à une communication en personne, au téléphone, ou aux examens cliniques, le cas échéant, ou encore à la consultation des urgences au besoin. Il appartient au patient d'assurer le suivi des communications électroniques du médecin et de prendre les rendez-vous qui s'imposent.
- Les communications électroniques relatives au diagnostic et au traitement peuvent être entièrement imprimées ou transcrites et faire partie du dossier médical. D'autres personnes ayant un droit d'accès au dossier médical, comme les membres du personnel et de la facturation, peuvent également avoir accès à ces communications.
- Le médecin peut réacheminer les communications électroniques à son personnel ou à d'autres intervenants concernés par la prestation et l'administration des soins. Le médecin peut utiliser un ou plusieurs Services pour communiquer avec ces intervenants. Cependant, le médecin ne peut réacheminer des communications électroniques à des tiers, y compris les membres de la famille, sans avoir préalablement obtenu le consentement écrit du patient, exception faite des cas autorisés ou exigés par la loi.
- Ni le patient, ni le médecin ne doivent utiliser les Services pour communiquer des renseignements médicaux délicats sur les sujets ci-dessous [cocher toutes les cases qui s'appliquent] :

  ☐ SIDA/VIH

  ☐ Santé mentale

  ☐ Déficiences développementales

  ☐ Abus d'alcool ou d'autres substances

  ☐ Autre (préciser) :
- Outre les sujets mentionnés au point précédent, le soussigné accepte d'informer le médecin de tout type de renseignement qu'il ne souhaite pas être abordé au moyen des Services. Le patient peut modifier cette liste en tout temps en avisant le médecin par écrit.

Paraphe du patient : _____

- Certains Services pourraient ne pas être utilisés dans certaines situations thérapeutiques ou pour communiquer des renseignements cliniques. Le cas échéant, l'utilisation de ces services se limitera à des communications à des fins éducatives, informationnelles ou administratives.
- Le médecin n'est pas responsable de la perte d'informations causée par des pannes techniques liées au logiciel ou au fournisseur de services internet du patient.

Instructions relatives à la communication au moyen des Services

Le patient qui communique avec son médecin au moyen des Services doit :

- Éviter autant que possible d'utiliser un ordinateur appartenant à son employeur ou à un tiers.
- Informer le médecin de tout changement apporté à son courriel, son numéro de cellulaire ou tout renseignement requis pour l'utilisation des Services.

Si les Services incluent les courriels, les messages texte ou les messages instantanés, le patient doit :

- Inclure dans l'objet de la communication une description appropriée de la nature de la communication (p. ex., « renouvellement d'ordonnance ») et son nom dans le corps du texte.
- Relire toutes les communications électroniques avant de les envoyer au médecin afin de s'assurer que les messages sont clairs et qu'ils contiennent tous les renseignements pertinents.
- S'assurer que le médecin est informé qu'il a reçu un courriel de sa part (p. ex., en envoyant une réponse ou en autorisant l'envoi automatique d'un accusé de lecture).
- Prendre les précautions requises pour respecter la confidentialité des communications électroniques, telles l'utilisation d'un écran de veille et la protection des mots de passe.
- Retirer son consentement uniquement par courriel ou en communiquant par écrit avec le médecin.
- **Le patient qui a besoin d'assistance immédiate, ou dont l'état semble grave ou se détériore rapidement, ne doit pas communiquer avec le médecin au moyen des Services**. Il doit plutôt appeler le cabinet du médecin ou prendre d'autres mesures appropriées, comme se rendre au service d'urgence le plus proche.
- Autres conditions d'utilisation en plus de celles détaillées ci-dessus (doit être paraphé par le patient) :

J'atteste, par la présente, avoir lu et pleinement compris les risques, conditions et instructions détaillés dans cette annexe.

Signature du patient

Date

Paraphe du patient : _____