EMAIL AND TEXTING

CASE STUDY 1 - OFFICE COMMUNICATIONS

A busy rural physician sets up an office email account and uses a smartphone for texting. The physician and her patients find electronic communication a boon, as many patients live a considerable distance from her office. Before leaving on vacation, the physician arranges for coverage by a locum tenens who will not be on call outside office hours. The physician informs the locum of the office email and her practice of answering questions daily. She leaves an out-of-office alert informing patients that she is on vacation and that a delay in response time is probable. She advises that patients who need a quicker response should telephone the office to make an appointment. The smartphone is shut off and left in the physician's locked desk drawer.

QUESTIONS

1. Do electronic communications present particular privacy concerns?
2. Did the physician do all she could to protect her patients' privacy?

DISCUSSION

This case study does not address who, besides the physician, has access to the computer and the email account. Nor does it discuss what information should be transmitted electronically, encryption or other privacy measures, such placement of the monitor. The CMA's *Physician Guidelines for Online Communication with Patients*[1] recommend: "Given the possible range of uses for online communications, physicians should establish a protocol that describes how such communications will be incorporated into their practice. This protocol can be used as the basis to inform staff, patients and others of the limits and rules associated with the use of the information transmitted online." The guidelines go on to list issues that should be included in an online communications protocol.

The privacy issue raised by this case study is that patients were not notified that a locum tenens would cover the practice. Patients sending personal health information (PHI) by email would discover only afterward that the message would be read by someone other than their physician. Some patients might prefer to wait until their physician returns from vacation to address a health issue.

The locum is considered a member of the circle of care and usually one does not require explicit consent to share PHI within that circle. Principle 6 of the *Principles for the Protection of Patients' Personal Health Information*[2] states: "Physicians may infer a patient's consent to collect, use, disclose and access personal health information for primary therapeutic purposes (i.e., for the purposes of direct patient care and treatment)." However, in this instance, a pivotal member of the circle is replaced — in effect, the circle expands — and patients are not informed this will occur. Patients still believe their email will be read by their physician and are not given the opportunity to choose not to share PHI with a different doctor.

ANSWERS

1. Do electronic communications present particular privacy concerns?

   Electronic communications present particular privacy concerns because of the nature of the medium. Electronic formats make PHI faster and easier to access and copy. Once PHI is disclosed in an email message, the physician may no longer be the data steward, and he or she cannot control what the recipient does with the information. Electronic storage devices make it easier to store and transport, hence, lose multiple records.

2. Did the physician do all she could to protect her patients' privacy?

   The case study does not provide enough information to answer yes or no; it depends on the physician's electronic communications protocol. A sure way to ensure that patients will not disclose PHI to the locum if they do not wish to is to send an "e-blast" informing patients that their physician is going on vacation and another physician is providing care.

OTHER ISSUES

Turning the smartphone off, locking it in a drawer and not mentioning it to the locum suggests that the physician assumes the office and the smartphone's systems are integrated. This is not necessarily so, and patients who text to the smartphone account may not receive an out-of-office notification and, thus, be unaware that their physician is on vacation.

FACEBOOK

CASE STUDY 2 - PATIENT REQUESTS TO "FRIEND" THEIR PHYSICIAN

A middle-aged family physician opens a Facebook account, because his grandchildren have "pestered" him into doing so. The physician posts photos of himself at home, at work and on vacation. He posts photos of his wife, children, grandchildren and office staff. With his grandchildren's help he "friends" his children, grandchildren, staff members and colleagues who have Facebook accounts.

After a few weeks, the physician begins to receive friend requests from his patients. Not wanting to insult his patients, he accepts the requests. Afterward, the physician notices some patients' messages include health-related questions.

The physician does not visit his page regularly and he finds the Facebook notices, invites, pokes and instant messages irritating. He begins to ignore messages and notices.

QUESTIONS

1. Should the physician have set up a personal Facebook account?
2. Should this physician have posted the photos he did?
3. Should physicians friend patients?
4. What can a physician do to control who can find him or her on Facebook and limit the number of friend requests?
5. Should physicians answer health-related questions via instant messaging?
6. Should this physician review notices and messages more regularly?

DISCUSSION

Many people find social networking a quick and convenient way to maintain contact and remain current with family and friends. Anyone may use social networking; however, according to the CMA's *Social Media and Canadian Physicians: Issues and Rules of Engagement*,[3] a primary rule of engagement is, "Understand the technology and your audience." Although not imperative, it is advisable to keep one's personal and professional lives separate. "While such a separation is a fundamental tenet of the medical profession, social media blur such boundaries in ways that can enrich communications, but can also put physicians at risk."[3]

Physicians using Facebook are advised to establish both a personal and a professional page and decide beforehand who will have access to each. One should develop and publicize the practice's online communication protocol and social media policy.[1] "When using social media, physicians should endeavour to use the most stringent security and privacy settings available for the particular platform."[3] If patients send a friend request to a personal account, they can be referred to the office's communications protocol, its social media policy and be directed the physician's professional site.

The physician can limit access to his personal page, while allowing patients and colleagues access to his professional site. The professional site can contain information about the practice, general health information and links to other sites. However, "Identifiable patient information, including images, should never be posted online or shared in electronic communications of a general nature."[3] To communicate with colleagues, physicians can join professional networking sites.

Blending personal and professional accounts can lead to complications. For example, if a patient sends a message to his or her physician regarding an urgent medical need and the physician does not respond in a timely manner, then the patient may believe the physician behaved unprofessionally and unethically. "The same standards of professionalism that would apply in face-to-face physician–patient interactions also apply in electronic interactions."[3] Thus it is advisable to manage patients and friends' expectations: "Physicians should determine how these expectations will be managed and communicate clearly to patients what the office protocol is with respect to response times."[1]

It is advisable not to answer specific health-related questions on a social networking site. "Social networking sites cannot guarantee confidentiality. Anything written on a social networking site can theoretically be accessed and made public."[3] By asking specific questions about their health, patients disclose PHI; but this does not give data stewards license to disclose that information. One should not assume patients know that posts to a social networking site are public.

ANSWERS

1. Should the physician have set up a personal Facebook account?

   There is no reason why physicians should not have personal Facebook accounts. However, it is advisable to limit access to personal accounts to family and friends and allow open access, e.g., to staff, patients and colleagues, only to professional accounts.

2. Should this physician have posted the photos he did?

   This depends. One certainly may include photos of family and friends on one's personal pages. Staff photos would best be posted on one's professional page and certainly only after obtaining explicit consent from staff.

3. Should physicians friend patients?

   Yes and no. Yes, certainly friend any patient at the professional account. If the patient is a personal friend, then friend them on one's personal account. All patients should receive a copy of the office's online communications protocol and social media policy so that boundaries are not crossed.

4. What can a physician do to control who can find him or her on Facebook and limit the number of friend requests?

   Use the most stringent security and privacy settings.

5. Should physicians answer health-related questions via instant messaging?

   This depends on the questions being asked. As confidentially cannot be guaranteed, it is best only to answer general health-related questions. If a patient asks specific questions about his or her health, it is advisable to ask the patient to book an appointment and inform the patient this is necessary to protect privacy and PHI.

6. Should this physician review notices and messages more regularly?

   Because this physician only has one account and he has friended patients who post health-related questions, yes it would be advisable to do so — at least until he establishes a professional account and his patient-friends migrate to it.

CASE STUDY 3 - CIRCLE OF FRIENDS AND PROFESSIONALISM

An ER resident is at the top of her class and has amassed an exceptional number of volunteer hours. The resident has a personal Facebook account. She posts personal information, her likes and dislikes, commentaries and assessments of her instructors' and classmates' knowledge and skills, writes about her good and bad days of residency and posts photos of herself, her friends and classmates enjoying themselves at social events. She has set no limitations on who can view her Facebook pages, posts and photos. The dean of medicine calls the resident to her office threatening discipline, perhaps suspension, for unprofessional conduct.

QUESTIONS

1. As a resident, how can she be charged with unprofessional conduct?
2. What did the resident do that may be considered unprofessional?
3. Should Facebook pages be considered public or private domain?
4. Is there a difference between personal and private?
5. If there is a difference, what is the significance for the resident?
6. What can the resident do to limit damages?

DISCUSSION

Social networking, search engines and the web are blurring the lines between public and private. Many conflate personal with private; they believe their personal site is private. But personal information is "broadcast" on social networking sites. A Facebook profile appears in the public domain, i.e., anyone can view it. If not restricted by privacy settings, posts intended for friends and family may be viewed by anyone. Posts intended for friends and family may, if not restricted by privacy settings, be view by anyone. Personal only becomes private when one decides to limit what is shared and with whom. "In order to use social media effectively, it is necessary to have a good understanding of how they work and who your intended audience will be before using them."[3]

Even applying the most stringent privacy settings does not guarantee that information is not widely available. Deleting a post does not provide surefire protection. Once posted, information is almost certainly stored somewhere in cyberspace; hence, in theory, permanently accessible. Before posting, consider how others may interpret what you post; for example, photos of drunken debauchery may not play well with someone hiring an emergency room physician. If there is something that some people do (or should) not need to know about you, avoid putting it online at all.

Medical residents are medical professionals and are subject to medicine's ethical and professional standards. The preamble to the *CMA Code of Ethics*[4] states that it is "an ethical guide for Canadian physicians, including residents, and medical students." All CMA policies are applicable to medical students and residents. The preamble to *Principles for the Protection of Patients' Personal Health Information*[2] states that they are intended as a resource for physicians (including medical students and physicians in training). Therefore, the resident is held to the same standards as practising physicians. "When communicating through social media, physicians must remember they remain governed by the same ethical and professional standards that have always applied and that are paramount."[3]

The content of the resident's postings to Facebook determines whether she acted unprofessionally. If the resident wrote disparaging remarks about her instructors or classmates, she may have transgressed paragraph 48 of the *Code of Ethics*[4]: "Avoid impugning the reputation of colleagues for personal motives; however, report to the appropriate authority any unprofessional conduct by colleagues."

ANSWERS

1. As a resident, how can she be charged with unprofessional conduct?
   Medical residents are held to the same standards as practising physicians.
2. What did the resident do that may be considered unprofessional?
   The answer depends on the content of the comments and photos.
3. Should Facebook pages be considered public or private domain?
   Information on Facebook pages should be considered personal, but in the public domain.
4. Is there a difference between personal and private information?
   Yes. Personal information is information that individuates someone. What makes personal information private is when access is controlled, i.e., it is not shared with everyone.
5. If there is a difference, what is the significance for the resident?
   The significance for this resident is that she apparently assumed personal meant private and posted inappropriate statements or photos and was, thus, accused of unprofessional conduct.
6. What can the resident do to limit damages?
   She can delete the inappropriate statements or photos and apologize. There is no guarantee the statements or photos are not still discoverable, as a friend might have copied them.

OTHER ISSUES

Residents' relationships with classmates and instructors are considered professional. A characteristic of professional relationships, whether physician–student, patient–physician, physician–nurse or physician–physician, is that they are circumscribed and particular behaviour is expected. Acting as if one's personal social networking site is private when it is not makes violating boundaries easy and highly likely.

CASE STUDY 4 - PATIENT ACCOUNTS AND PHYSICIAN REQUESTS TO "FRIEND" A PATIENT

A surgical team has a policy of not performing cardiac surgery on patients who continue to smoke. Mr. Gyles is scheduled for open heart surgery. The cardiologist informs Mr. Gyles that the team does not operate on smokers and asks him if he smokes. Mr. Gyles assures the cardiologist that he quit smoking a while ago. However, the cardiologist is suspicious.

The cardiologist searches online and finds Mr. Gyles' Facebook page. The cardiologist sends Mr. Gyles a friend request, which he accepts. The cardiologist subsequently scrolls through Mr. Gyles' page and finds photos of him smoking. The cardiologist notes her discovery in Mr. Gyles' medical record. The office manager telephones Mr. Gyles to inform him that his surgery may be cancelled. Mr. Gyles calls the cardiologist demanding to know the reason, and the cardiologist mentions the photos posted on Facebook. Mr. Gyles states that all the photos on Facebook are more than three months old; insists he told her he quit "a while ago"; and accuses the cardiologist of lying, spying and

transgressing his privacy rights. Mr Gyles questions the team's professionalism and informs the cardiologist that he may report her and the team to the provincial college of physicians and surgeons.

QUESTIONS

1. Should the cardiologist search for information about Mr. Gyles online?
2. Should the cardiologist ask to friend Mr. Gyles?
3. Should the cardiologist note in the medical record her belief that Mr. Gyles still smokes?
4. Should the cardiologist remove the entry?

DISCUSSION

"Trust plays a central role in the provision of health care and treatment; fulfilment of physicians' fiduciary obligations enables open and honest communications and fosters patients' willingness to share personal health information" (Principle 1[2]). The cardiologist's actions demonstrate a lack of trust. She does not believe Mr. Gyles' claim that he no longer smokes.

The cardiologist should address this issue directly with Mr. Gyles, as open and honest communication is usually best. She should consider her motives and the appropriateness of seeking information online. As noted, the cardiologist's actions could be considered an invasion of privacy, as she was not entirely truthful about why she asked to friend Mr. Gyles. Mr. Gyles was not told that the cardiologist wanted access to his Facebook page to gather health information. "It is advisable to ensure that patients know the rules and limits of online communications and, where possible, formally consent to these conditions."[1]

ANSWERS

1. Should the cardiologist search for information about Mr. Gyles online?

   No, as the veracity of the information cannot be substantiated without asking the patient.
2. Should the cardiologist request to friend Mr. Gyles?

   In this instance, no, as the cardiologist used Mr. Gyles' Facebook page to surreptitiously gather personal information.
3. Should the cardiologist note in the medical record her belief that Mr. Gyles still smokes?

   As the Facebook photos were not dated, her suspicion that Mr. Gyles still smokes is just a belief; suspicions should not be entered into the record as "objective" truth.
4. Should the cardiologist remove the entry?

   No, entries should not be removed. Mr. Gyles' refutation of the cardiologist's belief should, however, be included in the record.

Other Issues

"However, physicians must retain the appropriate boundaries of the patient–physician relationship when dealing with individual patients. The same standards of professionalism that would apply in face-to-face physician–patient interactions also apply in electronic interactions."[3] Because these vignettes primarily deal with privacy and confidentiality, other professional and ethical issues are not addressed in depth.

Case Study 5 - Office Staff Use of Social Media

A physician and her receptionist, Mr. Quan, are friends, i.e., they socialize after hours. When Mr. Quan invites the physician to be his Facebook friend, the physician accepts and visits Mr. Quan's page. The physician notices photos taken at the office and sees patients listed as Mr. Quan's friends. The physician notes that some patients post general health questions and commentaries about the physician and her practice. The physician is pleased that all comments are positive. However, she is surprised to see patients contacting Mr. Quan through Facebook to schedule appointments and ask about test results.

Questions

1. Should the physician accept Mr. Quan's invitation?
2. Should the physician be concerned about Mr. Quan answering Facebook friends' general health questions?
3. Should the physician be concerned that patient-friends contact Mr. Quan through Facebook to schedule appointments and ask about test results?
4. Are there any other concerns the physician should discuss with Mr. Quan?

Discussion

As discussed in case study 2, it is advisable to keep one's personal and professional lives separate. However, there are instances where this may be impossible: for example, physicians residing in small rural communities. "Social media pose a challenge for physicians (and other professionals) in terms of separating one's personal and professional lives."[3] Associating with employees after work or through social media can present boundary issues, but conflicts should be manageable.

Mr. Quan may not be aware of or is not managing boundary issues. All health care professionals and workers are beset with health-related questions while attending social events. If the questions are general and generalizable answers are provided, then no therapeutic relationship is established. "Physicians should take care to avoid appearing to provide medical advice to non-patients and inadvertently establishing a patient–physician relationship through the exchange of information."[1]

It is advisable that allied health professionals and staff follow this advice. The physician could make Mr. Quan aware of boundary issues: the potential for inadvertently breaching confidentially and transgressing patient-friends' confidentiality by answering health-related questions on his personal Facebook page. For example, the physician could explain how a response to a question about the availably of a particular test result could break confidence and breach privacy.

If the physician does not have a policy on online communication with patients, one should be developed,[1] as patients correspond with Mr. Quan to schedule appointments.

As the physician's staff use social media for personal and professional purposes, the online communications policy could stipulate that employees establish a professional Facebook account. "Physicians with employees should make them aware of issues concerning patient confidentiality in their own use of social media. Consideration should be given to instituting a social media policy for the office or practice."[3] Then Mr. Quan could ask patient-friends to contact him through his professional site to book appointments. "To differentiate communications with physicians from communications with office staff, separate email accounts or online options can be used and patients should clearly understand when to use which address."[1]

ANSWERS

1. Should the physician accept Mr. Quan's invitation?

   If both respect the personal–professional boundary, then yes.
2. Should the physician be concerned about Mr. Quan answering Facebook friends' general health questions?

   If Mr. Quan's responses are generalizable, there is no need for concern. If, however, Mr. Quan discusses personal health issues, then the physician should remind him about the danger of breaking confidence and breaching privacy.
3. Should the physician be concerned that patient-friends contact Mr. Quan through Facebook to schedule appointments and ask about test results?

   Probably, as this elevates the risk that Mr. Quan could inadvertently break confidence and breach a patient's privacy.
4. Are there any other concerns the physician should discuss with Mr. Quan?

   Yes, they should discuss developing an office online communications policy, boundary issues and whether Mr. Quan should develop a professional Facebook page that patient-friends can use to book appointments. The physician should discuss with Mr. Quan the risk to patients' privacy posed by answering personalized health questions on Facebook.

TWITTER

CASE STUDY 6 - COMMUNICATING MEDICAL ADVICE

A palliative care physician tweets and receives responses from family, friends, colleagues, strangers and a few patients. Some responders ask specific health questions related to their or their loved one's medical condition. The physician knows that, if he is not careful in crafting his answers, he could inadvertently disclose confidential PHI.

QUESTIONS

1. If a patient publicly discloses PHI, does this absolve physicians of their obligation to keep PHI confidential?
2. What other professional issues should tweeting physicians be aware of and manage?

DISCUSSION

"Identifiable patient information, including images, should never be posted online or shared in electronic communications of a general nature."[3] A patient's decision to publicize or disclose personal information is not equilivant to granting a physician a waiver or absolution of the obligation to keep PHI confidential. Paragraphs 34 and 35 of the *Code of Ethics*[4] exhort physicians to "Avoid public discussions or comments about patients that could reasonably be seen as revealing confidential or identifying information" and "Disclose your patients' personal health information to third parties only with their consent, or as provided for by law." Posts to social media should be treated as public broadcasts.

"Social networking sites cannot guarantee confidentiality. Anything written on a social networking site can theoretically be accessed and made public."[3] Unless the respondent or patient consents to disclosure of PHI for secondary purposes not privileged by legislation, PHI should remain confidential.

"As a physician you can often bring most value to a forum or conversation by discussing issues on which you have a particular expertise. Sharing this information — as long as it does not contravene individual patient confidentiality — raises the level of discourse on social media sites and is likely to be viewed favourably by other participants."[3]

Protecting privacy is not the only professional concern physicians should be aware of. If a question is asked and the physician responds, the issue of establishing a doctor–patient relationship arises. "Physicians should take care to avoid appearing to provide medical advice to non-patients and inadvertently establishing a patient–physician relationship through the exchange of information."[1] The physician should craft his replies such that it is evident no patient–physician relationship has been established.

"While use of social media could potentially increase the exposure of physicians to disciplinary and medico-legal issues, those physicians who choose to use social media can help shape how these tools can improve health care in the future."[3]

"You should anticipate that the information you provide on social media may be challenged by both other physicians and non-physicians. Remember to keep the tenor of the debate at a civilized level and do not be unnecessarily offended if your viewpoint is rejected, even if you do feel it is based on best available evidence."[3] A good debate addresses the issues; it does not degenerate into personal attacks. Given that digitized communications are easily manipulated and shared comments are easily taken out of context; authors should temper comments. "The same piece of information can be sent to and stored in numerous places, readily linked to other pieces of data and efficiently used for purposes unintended at the time of original collection."[1]

Answers

1. If a patient publicly discloses PHI, does this absolve physicians of their obligation to keep PHI confidential?

   A patient's public disclosure of PHI does not absolve physicians of the obligation to keep PHI confidential; the obligation is owed to the patient and only the patient may waive the obligation via expressed or implied consent. Public disclosure is not sufficient to infer consent; therefore, relying on implied consent is insufficient.

2. What other professional issues should tweeting physicians be aware of and manage?

   The physician should be aware that by sharing medical information, there is a risk that a patient–physician relationship could be established; a relationship that imposes professional obligations to which the physician will be accountable.

Blogs

Case Study 7 - Physicians' Blogs

An intensive care unit physician blogs under her own name. In one post, she discusses an adverse event, the harm caused, lessons learned and subsequent changes that mitigate risks to patient safety. The physician is careful not to name the patient or the hospital; however, in previous posts, she has mentioned her specialty and her hospital.

Questions

1. Is this a primary or secondary use of de-identified PHI?
2. Should the physician obtain her patient's consent to blog about the event?
3. Could the patient be identified through the blog?
4. If the patient could be identified, how could this happen?
5. Would blogging under a pseudonym protect patient privacy?
6. What can physicians do to limit the risk of breaching patient privacy when posting information on a social networking site?

Discussion

"More frequent communication with patients and the public improves the quality of medical care and satisfaction with physician care. Social media can enhance the role of traditional media in delivering important public health messages."[3] Every act has potential benefits and risks of harm. The magic is finding the right balance. In this case, improving patient safety must be balanced against the risk of transgressing patient's privacy rights.

Paragraphs 31 and 34 of the *CMA Code of Ethics*[4] exhort physicians to "Protect the personal health information of your patients" and "Avoid public discussion or comments about patients that could reasonably be seen as revealing confidential or identifying information." If the information is obtained and disclosed for purposes other than providing direct patient care and treatment, then the use should be classified as a secondary purpose. Making PHI anonymous allows access to it and its use by physicians, researchers and data stewards, as its source is no longer identifiable and privacy is purportedly protected. "Physicians may exercise discretion when the use or disclosure of personal health information without consent is permitted, but not required by law" (Principle 10[2]). Because this is a secondary use of PHI, not privileged by legislation even if made anonymous, the physician should consider obtaining the patient's consent as there is a risk of identification.

The more details provided, the easier it is to re-identify a patient. For example, including the date of an adverse event, what and how it happened, the name of the hospital, the patient's condition and the harm suffered would allow identification of the patient. If the physician discloses to the patient the potential for identification when she obtains the patient's consent to use his or her information, then she may have limited her liability for breaching her fiduciary duty to keep PHI confidential.

Even blogging under a pseudonym does not guarantee patient anonymity. An interested and persistent person could trace the anonymous blog back to the blogger. "Electronic communications are not anonymous and are always stored in some form. As such, it is possible to trace the author of a comment even if posted anonymously."[3]

Once something is posted, the author cannot control dissemination or how long the post is stored. "The same piece of information can be sent to and stored in numerous places, readily linked to other pieces of data and efficiently used for purposes unintended at the time of original collection."[1] If, however, the patient understood the risks and consents to the use of de-identified information, the proper balance between societal interests and personal rights may be achieved.

ANSWERS

1. Is this a primary or secondary use of de-identified PHI?

   This is a secondary use, as the data are not used for direct therapeutic purposes. (See Circle of Care vignette, case study 4.)

2. Should the physician obtain her patient's consent to blog about the event?

   Even though the information has been de-identified, PHI is used for a secondary purpose — not subject to a legal waiver — and will become public; thus, it is advisable to obtain the patient's express consent.

3. Could the patient be identified through the blog?

   Potentially, yes. It depends on how many specific details are included. The more information available, the easier it is to identify a particular person.

4. If the patient could be identified, how could this happen?

   If someone conducts an online search using the name of the hospital, the physician and the term "adverse event," the information contained in current and past blogs could be sufficient to identify the patient.

5. Would blogging under a pseudonym protect patient privacy?

   Not necessarily. Anonymity (de-identification) is a function of the specificity of the information and how much information is available. In short, combining all available information can result in identification.

6. What can physicians do to limit the risk of breaching patient privacy when posting information on a social networking site?

   Physicians can change case information or delay publication so that data linking is difficult.

CASE STUDY 8 - PHYSICIANS' ADVOCACY

A salaried emergency room physician works in an ER that is, as most are, overcrowded and short-staffed. It has long wait times and is running at 110% occupancy. There are always four or five patients in beds in the hallway awaiting admission. With impending budget cuts, hospital administration decides to close the diabetic out-patient clinic. The physician fears closure will place additional stress on the ER; the clinic's patients will begin to rely on the ER for care of ulcerated feet, for example. The physician blogs about the clinic's closure, the potential adverse impact on the ER and its consequences for patients. The hospital's CEO is angry that the physician blogged about the clinic's closure and threatens sanctions as the physician transgressed the hospital's media policy.

QUESTIONS

1. Should the physician publicize the hospital's decision to close the diabetic clinic?
2. Is the CEO's threat tantamount to a gag order?
3. Are there privacy implications?

DISCUSSION

Most institutions have media policies that identify an official spokesperson. Given the popularity of social media and the fact that posts to the web are public, institutions likely have a social media policy. "If a physician is an employee of a health care institution or organization that has social media guidelines in place, he or she should review these and act accordingly."[3] Rightfully, institutions are concerned with their public image. "If you are employed by an institution or organization, you should state either that you are reflecting corporate policies or that the views expressed are yours alone and not those of your employer."[3]

However, the institution's interests should not trump an individual's right to free speech. Therefore, institutions' policies should not be so stringent as to be tantamount to "gag orders." Physicians are obligated to advocate for their patients' well-being and "Recognize the responsibility of physicians to promote equitable access to health care resources" (Paragraph 43[4]). The institution's interest in protecting its public image must be balanced with individual rights and employees' professional obligations.

Writers should, however, remember that their right to free speech is not a licence to say anything; there are limits to free speech. "Postings to social media sites are subject to the same laws of copyright, libel and defamation as written or verbal communications."[3]

Ideally those affected by a policy will be involved in developing it or will be represented by someone who advocates for their interests. Thus, for example, if a hospital's media policy does not address everyone's privacy rights, physicians should petition for an inclusive policy.

ANSWERS

1. Should the physician publicize the hospital's decision to close the diabetic clinic?

   As the patients of the hospital will be adversely affected by the decision, his blogging about the decision could meet his obligation to advocate for his patients' well-being.

2. Is the CEO's threat tantamount to a gag order?

   With the information provided, this is difficult to answer. Certainly, the physician should be aware of and follow the hospital's media and social media policies when blogging. Sometimes, however, one should become a whistleblower and inform those who are or will be adversely affected.

3. Are there privacy implications?

   If no PHI or "company secrets" are revealed and no violation of hospital privacy policies occurs, then probably not.

VIDEO AND IMAGES

CASE STUDY 9 - POSTING VIDEO OR PHOTOS TO THE WEB (YOUTUBE, INSTAGRAM)

To meet requirements for an elective, a resident makes a video showing how to insert a central line. The resident recruits a patient and explains that he will ensure she cannot be recognized as her face will be "masked" in post-production and any physical attributes that could identify her will be air brushed. The patient consents with the understanding that the attending physician, the instructor and the resident's classmates will view the video; all are members of the patient's circle of care.

In the video, the resident identifies himself, his specialty, the patient's condition and the year and provides a running commentary. The patient's face is masked in post-production and any physical attributes that could identify the patient are air brushed.

The resident receives high marks for the video and is praised by the attending physician, the instructor and his classmates. All urge him to post the video to the hospital's website and YouTube. The resident posts the video on both sites.

QUESTIONS

1. What, if any, concerns are there with the consent process?
2. Should the resident post the video online?
3. Could the video (or photos) become publicly accessible?
4. Are there any privacy concerns?
5. Is discussing the patient's condition a primary or secondary use of PHI?

DISCUSSION

Some may argue that the resident was not required to disclose and obtain the patient's consent to share the video, because he can rely on implied consent for sharing PHI with the health care team. "Under certain circumstances, physicians may rely on a patient's implied informed consent to share personal health information" (Principle 6[2]). Also, "The use or disclosure of patient information within the 'circle of care' should be done solely on a need-to-know basis" (Principle 8[2]).

If, as in this case, the resident shares the video without the patient's explicit consent, he will have contravened both principles. Why? Because the information is not being shared for a therapeutic purpose, i.e., the patient would not directly benefit. As the commentary to Principle 8 notes: "This principle limits the sharing of personal health information with members of the health care team to only that information which is necessary for each team member… to provide the patient with direct health care and treatment." If use or disclosure of a patient's PHI does not directly benefit the patient, then it is considered secondary, i.e., education. Disclosing PHI to third parties without explicit consent for such a secondary purpose is not permitted by law; therefore, obtaining the patient's explicit consent is required.

In this case, the original intent was that members of the patient's circle of care would see the video for educational purposes. It is doubtful that the prior consent obtained is sufficient to allow posting to the hospital's website and YouTube. The patient was not informed of and did not consent to posting of the video online. Also, as the resident did not discuss his plan to provide a running commentary that included the patient's condition, disclosure was inadequate and, thus, the validity of the consent is questionable.

Because the resident identified himself, his specialty, the year, the hospital and the patient's condition, this information may be sufficient for someone to identify the patient; thus, patient privacy could be breached. It is advisable for the resident to show the patient the video before others see it and, if his plans change, re-contact the patient, disclose the risk of identification and seek explicit consent to post the video to the hospital's website and the web. In this case, given the risk of identification, it may be advisable not to post the video. As stipulated in the CMA's social media policy: "Identifiable patient information, including images, should never be posted online or shared in electronic communications of a general nature."[3]

"Social networking sites cannot guarantee confidentiality. Anything written on a social networking site can theoretically be accessed and made public."[3] How limited-access photos become publicly accessible was not directly addressed in the case study. However, those using digitized, electronic platforms should be aware that "The digitized nature of e-communications facilitates rapid and easy

sending, storing, sharing and searching."[1] Once access is granted, the author of the post no longer controls further dissemination.

"Patients should be informed that the treating physician cannot control access and guarantee confidentiality for an electronic health record (EHR) system" (Principle 13[2]). The same disclosure should occur if the intent is to post patient images and information on the web.

ANSWERS

1. What, if any, concerns are there with the consent process?

   First, the patient may not have been adequately informed; the resident did not disclose his plan to mention the patient's condition in the commentary. Second, when plans changed, the resident should have re-contacted the patient and obtained explicit consent to post the images.
2. Should the resident post the video online?

   Given he did not obtain the patient's consent to post the video, the elevated risk of identifying the patient and of non-consensual disclosure of PHI to third parties, he should not have posted it online.
3. Could the video (or photos) become publicly accessible?

   Yes, someone could copy and post the video (or photos) to other websites. The copies could include embedded information, such as date, time and location.
4. Are there any privacy concerns?

   Given the information contained in the video, the patient might be identifiable. The risk of identification is magnified as the video is on the website of the treating hospital. The risk is even greater if the hospital has a small or rural catchment area.
5. Is discussing the patient's condition a primary or secondary use of PHI?

   This is a secondary use of de-identified PHI.

References

1. *Physician Guidelines for Online Communication with Patients*. Ottawa: CMA; 2005. Available: http://policybase.cma.ca/dbtw-wpd/PolicyPDF/PD05-03.pdf (accessed 2012 Sept. 12).
2. *Principles for the Protection of Patients' Personal Health Information*. Ottawa: CMA; 2011. Available: http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf (accessed 2012 Sept. 12).
3. *Social Media and Canadian Physicians: Issues and Rules of Engagement*. Ottawa: CMA; 2011. Available: http://policybase.cma.ca/dbtw-wpd/Policypdf/PD12-03.pdf (accessed 2012 Sept. 12).
4. CMA Code of Ethics (update 2004). Ottawa: CMA; 2004. Available: http://policybase.cma.ca/dbtw-wpd/PolicyPDF/PD04-06.pdf (accessed 2012 Sept. 18).