ASSOCIATION MÉDICALE CANADIENNE CANADIAN MEDICAL ASSOCIATION

CMA POLICY

PHYSICIAN GUIDELINES FOR ONLINE COMMUNICATION WITH PATIENTS

INTRODUCTION

The increased availability and use of the Internet have facilitated online communication between physicians and patients when the patient is not physically present at the physician's place of practice. Online communications may be directly related to the provision of patient care or may be used for transmitting more general information for administrative, educational or health promotional purposes. These guidelines are primarily concerned with the two most common vehicles of online communications: email and physician web sites.

Electronic communications offer many benefits, but require safeguards that differ from other forms of communication, such as paper document, telephone and fax. The digitized nature of e-communications facilitates rapid and easy sending, storing, sharing and searching. However, these inherent benefits create challenges related to the preservation of privacy and confidentiality. 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.

To the extent possible, privacy and confidentiality should be maintained at a level that is comparable to that currently expected for the paper record. Physicians should refer to the CMA's *Health Information Privacy Code* and *Code of Ethics,* as well as specific laws or requirements in their jurisdiction for guidance in this respect.

These guidelines take as their starting point norms and best practices that have developed through the use of paper documents, mail, telephone and facsimile in the setting of physicians' offices. They also take account of the unique challenges posed by digitization and online communication as well as their potential to open up new avenues to facilitate the provision of care and the dissemination of information. This guide does not address physician communications with other health care providers, government and other third parties.

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 protocol should address all of the following:

a. Purposes for which the office uses online communications
b. Online (distant) patient–physician relationship
c. Response to patient enquiries — managing

Correspondence and requests for additional copies should be addressed to the Member Service Centre, Canadian Medical Association, 1867 Alta Vista Drive, Ottawa, ON K1G 3Y6; tel 888 855-2555 or 613 731-8610 x2307; fax 613 236-8864.

All policies of the CMA are available electronically through CMA Online (www.cma.ca).

expectations
d. Conditions for patient use of online communications
e. Triage of communications
f. Access to patient enquiries
g. Retention, form and organization of communications
h. Type and quality of information provided to patients
i. Privacy, confidentiality and security
j. Specific jurisdictional provisions and requirements

Each of these topics is discussed in more detail below. In addition, specific technical issues should be addressed, and a checklist and overview are provided for this purpose (Appendix A).

GUIDELINES

a. Purposes for which the office uses online communications

The following is a range of potential uses for online communications. Physicians should ensure that they communicate only those specific uses that have been adopted by their practice.

Administrative uses

- Scheduling appointments (including rebooking and cancellation)
- Online payment for non-insured or otherwise insured services
- Providing directions (to the practice location and other facilities)
- Providing practice policies and protocols (e.g., privacy policy, non-insured billing guidelines, protocol for third-party request)

Education and health promotion

- Providing general educational and health promotion electronic documents and resources
- Providing links to educational and health promotion web sites
- Incorporating health promotion messages
- Providing links to online self-assessment and help tools
- Providing guidance to patients regarding health-related web sites
- Newsletters and alerts
- Community support resources

Patient care

- Receiving patient requests for prescription refills
- Clarifying or reiterating instructions
- Receiving and answering patient follow-up questions
- Providing post-procedure instructions and follow-up
- Notifying or reminding about routine tests and procedures
- Monitoring
- Providing test results (where acceptable)
- Consulting related to conditions that have been previously discussed
- Consulting related to new conditions

b. Online (distant) patient–physician relationship

In any online (or distant) communication, physicians should be guided by their professional obligations to the patient, which will continue to be just as stringent in the online world.

Existing patients of the physician: Most online communications will be between physicians and existing patients. Physicians should establish a mechanism to ensure that they are communicating with registered patients within the context of a patient–physician relationship.

Non-patients: 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. Devices such as notices on open web sites describing who the information on the site is for, the use of closed (password protected) web sites and a standard automated response to non-patients can be used to this end.

Prospective patients: In some instances, for example referral and new patients, physicians may want to establish preliminary communications electronically for such purposes as:

- Setting up an appointment
- Acquiring preliminary information, such as patient contact information and basic medical history
- Providing basic information about the office visit

In these instances and despite the fact that no patient–physician relationship has been formed in person, it is advisable to ensure that the patient has agreed to the conditions and limits of online communications. If any preliminary medical information is provided via this route, it should also be made clear that this will only be reviewed when the patient attends his or her first appointment. Instructions should also be given to the patient with respect to alternative means to obtain treatment should the need arise before the first appointment.

Virtual[1] *patients:* Currently, a variety of guidelines appear to discourage or forbid a purely online or virtual patient–physician relationship. Emphasis is generally placed on the importance of face-to-face, in-person encounters and the use of electronic communications only as a means of follow-up, clarification, monitoring, etc., within the context of an existing relationship. However, through telehealth technology, clinicians have been developing practice protocols that are allowing them to provide care at a distance. This is an emerging field and, as the sophistication of technology and the users of it increases, then the current reluctance may well be revisited. This may be especially so in cases where physical access to a physician is severely limited or non-existent (for example, in remote or emergency settings) and the benefits of a virtual relationship are demonstrably better than no access at all.

c. Response to patient enquiries — managing expectations

Patient expectations about how quickly a physician or the physician's office will respond to their enquiries online may be unrealistic. Physicians should determine how these expectations will be managed and communicate clearly to patients what the office protocol is with respect to response times. The following mechanisms might assist in clarifying and communicating expectations, and generally managing email traffic.

- Establish reasonable response times — different enquiries may warrant different response times; account for responses during times of practice closure (weekends, vacations, statutory holidays)
- Automatically acknowledge receipt of communications and indicate the protocol for response
- Provide instructions about access to alternatives in case of emergency or urgent situations
- Encourage or require the provision of a subject heading
- Triage messages according to subject heading and establish a procedure for responding to each type
- Limit time required to read and respond to patient communications by encouraging or requiring limited text from patients; restricting communications to single or simple issues; encouraging or requiring office visits for complex matters
- Use templates to encourage or require standardized communication (with possible benefits regarding storage and linkage)
- Publicize response times (on the physician's web site, in an automated reply, in initial instructions to patients, in an agreement with patients); include instructions regarding emergencies or urgent instructions or in the event a response is not received within the specified time

d. Conditions for patient use of online communications

It is advisable to ensure that patients know the rules and limits of online communications and, where possible, formally consent to these

[1] This term has been used to describe a patient who has never been seen by a physician but who is nevertheless in a patient–physician relationship with the physician.

conditions. Written consent could be obtained via an appropriate click-consent online, provided the physician has a mechanism to authenticate the identity of the person consenting. Provision should be made for patients who have questions to discuss the issues with their physicians before providing consent.

Conditions of use might include:

- Acknowledgement of the permitted purposes of online communications and agreement to use online communications only for those purposes
- Knowledge of and consent to office staff's access to online communications
- Acknowledgement of the alternative sources of communication in specific circumstances, such as emergency or no response
- Agreement to abide by established protocols with respect to such matters as subject headings, length of text and use of templates
- Verification of the patient's email address and agreement on the patient's responsibility to prevent unauthorized access to his or her own system
- Recognition and acknowledgement of the insecure nature of online communication
- Recognition that the communication might become part of the patient's record
- Agreement to refrain from using offensive language
- Agreement to refrain from using online communication for frivolous or commercial purposes
- Acknowledgement that permission to use online communication may be withdrawn for failure to abide by the terms and conditions of use
- Agreement to receive periodic communications from the physician with respect to such matters as drug recall, alerts, health promotion and disease prevention
- Agreement to pay a fee to use the online capacity (in situations where online communication is not an insured service)

e. Triage of communications

To allow for efficient administration of patient communications, patients should be encouraged or required to use standard subject headings to describe the type of enquiry. If communication is occurring via the physician's web site, this could be accomplished using a pull-down menu. If communication is occurring via email, an automated or manual reply may be used to respond to communications that do not comply with the standardized format. The response should include the list of standardized subject headings. Patients should be advised that if they do not receive a reply to their communication, they should assume that the email was not received.

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. A clear procedure for routing communications within the office should be established so that all messages are attended to by the responsible person within an appropriate time.

Physicians will need to consider the problem of unwanted, unsolicited communications (spam). A variety of products are available to filter out unwanted messages. However, care must be taken to ensure that legitimate messages are not inadvertently deleted or denied access to the physician's system.

f. Access to patient enquiries

Unlike the private conversations that patients conduct with physicians in the office, online communications are open to others. The protocol should address the following issues.

- Will the physician be the only person who receives the patient enquiry or is the protocol open to other physicians in the office (for example, to facilitate on-call)?
- If office staff are the first point of contact, provide guidance as to how messages intended for the physician are to be addressed, routed and stored and ultimately replied to
- Because patients may expect to be communicating directly with and only with the physician within the context of a private

"space," they should be made aware of the extent to which others have access to this communication and be advised that the nature of the communication itself (digitized, written and a complete record of the conversation) makes it more vulnerable to review by others.

g. Retention, form and organization of communications

All communications with patients will result in the formation of a number of records, including both paper and electronic records held by both the physician and patient. In determining what should be retained and in what form, physicians may want to keep in mind the record held by the patient and the need to retain a duplicate of that record to respond to the patient or others on a specific matter related to the record. Physicians should consider whether to abstract relevant portions of the communication or whether to simply attach the whole communication to the patient's file as an electronic or paper record.

In developing procedures around the retention and organization of electronic communications, physicians should first consult the regulatory requirements in their specific jurisdictions. As electronic communications and electronic patient files become more commonplace, it is likely that these requirements will also be updated; thus, a periodic review of the regulations is also desirable.

Consideration should be given to how the electronic and paper files will be organized and how they interrelate. Where relevant, consideration should be given to how electronic communications can be integrated into the electronic record.

h. Type and quality of information provided to patients

Online communications provide a vehicle for disseminating valuable information to patients for education, health promotion and clarification via a physician's web site or email. In selecting the type of information (or web link) to provide, the physician should

- Ensure that the patient is advised that the information is for general purposes only and should not be perceived as the medical advice of the physician. Patients should be encouraged to discuss their specific medical issues with their physician.
- Provide the patient only with material from (or links to) credible sources, such as peer-reviewed journals and specialty societies.
- Ensure that the information is current. Physicians may consider electronic mechanisms to help in this regard (for example, automatic removal of stale-dated material).
- Ensure that they are respecting copyright rules and are not disseminating information without the consent of authors or owners.
- When providing web links, make it clear that the user is leaving the physician's web site.

i. Privacy, confidentiality and security

Sensitivity of information transmitted and degree of security in place: The type of information transmitted via the Internet can range from the relatively benign (for example, an appointment time) to the highly sensitive (for example, a test result or diagnosis that may have adverse consequences). As a general rule, sensitive information should be transmitted via the Internet *only* if sufficient security mechanisms are in place to ensure privacy and confidentiality. The transmission of adverse test or examination results should be avoided; these should generally be given during a face-to-face encounter with the patient so that the patient can discuss the matter directly with the physician.

To some extent, sensitivity is a matter of the subjective knowledge, judgement and expression of the individual patient and it should not be assumed that all patients have the same view of what constitutes sensitive information. Patients should be advised of the types of communication that the physician will engage in via email and the security measures that the physician has in place. Patients should also be provided with an opportunity to specify their preferences with respect to information exchange via email and be advised as to whether these preferences can be accommodated.

Means of transmission: Electronic communication generally occurs via the Internet, a local area network or (increasingly) via wireless vehicles[2] and can be a more or less secure means of communication depending on how the communication is protected from being viewed by unintended eyes. Patients should generally be discouraged from receiving electronic communications at locations where others might retain a record or have access to the communication (for example, in the workplace).

Patients should be advised about office practice and to take whatever precautions they deem appropriate to maintain the confidentiality of their records on their home systems.

In the physician's office, privacy and confidentiality should be maintained at the same level currently provided or required[3] when communicating by paper document, telephone or fax.

To ensure an adequate level of security, encryption or password protection should be considered as well as the use of secure servers to post and retrieve communications.

Care should be taken to ensure that the chosen service provider can adequately protect the confidentiality of patient information in accordance with physician expectations, Canadian law and physician regulatory authorities. The jurisdiction (location) of the service provider should also be considered to ensure that all of the protections of Canadian and provincial or territorial law are applicable. (Appendix A provides further details on these technical matters.)

Interoperability, security and practicality: To use email to transmit all manner of information, it will be necessary to ensure that sensitive information (which includes medical information) can be transmitted in a secure fashion and, preferably, according to recognized and accepted standards of collection, use and disclosure. This is no easy task. Although a physician might implement a secure means of communicating with patients, the same means may not be a practical way to communicate with other health care providers. For example, a physician might implement encryption, which will entail providing each recipient with a key to access the information. As between physician and patient, this may be a practical solution, but between providers it might require each provider to know and implement multiple keys.

Verification and authentication: Care should be exercised to minimize the likelihood that the email communication is sent to the wrong address or received by the wrong recipient. Various mechanisms can be used to accomplish this, including

- Authentication techniques[4]
- Extracting email addresses from an electronic address book where they have been carefully entered (similar to the pre-programmed fax function)
- Strongly recommending that patients receive email at an email address that is password protected and only accessible by them (e.g., not at work)
- General procedures to double check the address before sending
- A statement on each email communication that provides for circumstances when an email is received by the wrong recipient.
- Not sending an email message to multiple recipients (e-blasts) and allowing each recipient to see who else has received the message (a breach of confidentiality)

Physical safeguards: The computer system used by the physician should be subjected to physical safeguards to protect the integrity of data stored and to reduce the risk of modification, loss,

[2] Particular attention to security of information should be given when using wireless devices (see Appendix A for further details).

[3] In some jurisdictions, regulators will have specific requirements with respect to communications via telephone, fax or email.

[4] Note that this may be challenging to implement.

access, disclosure or theft. Such mechanisms include

- Placing the computer system in a secure space
- Requiring the use of passwords and changing them regularly
- Ensuring that computer screens in the office are positioned so that they cannot be read by unauthorized people[5]
- Installing reliable anti-virus software and keeping it up to date
- Installing a firewall[6]
- Backing up the system regularly and, ideally, storing the back-up in a secure place in a different location from the practice
- When discarding old computer systems, ensuring that the hard drive is properly destroyed
- When discarding data stored on other media (e.g., CDROM, PDA), ensuring that all data elements are completely erased.

Updating or creating the office privacy policy: The office privacy policy should be updated to include reference to email use and the protections in place.[7]

j. Specific jurisdictional provisions and requirements

Canadian physicians are generally licensed to practise medicine within the jurisdiction of a province or territory and are restricted from practising beyond their licensed jurisdiction. When using electronic communications, care should be exercised to avoid practising medicine beyond the licensed jurisdiction. Statements in email and on a physician's web site can clarify the physician's intent in this regard and can also reduce liability regarding those claiming that they relied on the information provided by the physician.

[5] Other techniques to accomplish this end include installing a privacy screen over the computer screen.

[6] A combination of hardware and software designed to control the flow of information between computers and the Internet (source: *Digital defense: what you should know about protecting your company's asset* by Thomas J. Parenty, Harvard Business School Press, 2003.

[7] Physicians are advised to have an office privacy policy in place that is available to patients.

Appendix A – Security Issues Checklist [8]

Information security may require some specialist knowledge, but the approach is not all that different from how you maintain the physical security of your office. For example, when you installed the doors and locks on your premises, you probably considered the following factors:

- Usability
- Functionality
- Security
- Reliability
- Cost
- Maintenance

Your systems and network access are no different. Choosing and installing general software applications and specific information security measures requires the same calculation of factors and costs. The steps you take to ensure the physical security of your office probably seem like second nature. But they are a learned response to known threats and vulnerabilities. Locked doors and secure filing cabinets are all security steps that we take for granted. Securing our networks and information systems should be no different.

Just as with other purchases, good information security requires both initial effort and ongoing checks. You need to do your research before buying security software, hardware or maintenance services. While you should expect the technology to work well, you still need to carry out the right checks to ensure that it's working correctly. Appropriate features must be set and adapted to work with your existing computers, software and network connections. Many security vulnerabilities are created when people install a new application and simply leave all the default settings in place, making them much easier for unauthorized users to manipulate.

It may seem complicated or overwhelming at first, but over time your actions will become so familiar and automatic that they constitute a 'culture of security'. No one expects physicians to review software code or understand the intricate workings of hardware. But you can and should read the relevant information, ask pertinent questions and get explanations of issues that don't seem clear. By taking the initiative and showing that security is important to your office, you can go a long way to making sure that your information systems develop in a secure way. In some cases, for example when making significant changes to your information systems, you may need expert assistance in the initial configuration and deployment of the system. It is essential to keep asking the experts what they are doing and why, and to satisfy yourself that the choices made reflect your business needs and improve the information security of your business.

Even with limited resources and expertise, there is much you can do to help secure your IT system and network access. Consider the questions below. Are you taking these steps?

- Do you have a firewall on your computer if you have Internet access (especially broadband access)?
- Do you have software to detect and destroy viruses transmitted by e-mail or in documents?
- Is security an important criterion when you choose software or service providers?
- Do you understand the security functions of the software and hardware you already have?
- Has anyone in your office taken a computer course to become more familiar with these functions?
- If you have the resources and it's appropriate, have you consulted a local expert on the configuration and deployment of your IT system?
- Have you checked if there are resources or information from government, a local trade association or chamber of commerce that relate to computer security?

[8] The content of this Appendix is a condensed version of an OECD document entitled 'Information Security Issues and Resources for Small and Entrepreneurial Companies – A Business Companion to the 2002 OECD Guidelines for Security of Networks and Information Systems" prepared by the "International Chamber of Commerce".

- Have you taken steps to physically secure your computers, especially laptops and portable devices?
    - Do you regularly back-up data off-site? And test your back-ups?
    - Do you require your employees to use passwords?
    - Do the passwords used contain both letters and numbers?
    - Are passwords kept securely (not written down or shared, for example) and changed at least every three months?
    - Do you try to train your employees on information security?

What follows is a checklist of actions that you can take to improve the level of security for the information technology aspects of your office

Physical Security

- Fit appropriate locks or other physical controls to the doors and windows of rooms where you keep your computers.
- Physically secure laptops when they are unattended (for example, by locking them in a drawer overnight).
- Ensure that you control and secure all removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to your business-critical assets.
- Make sure that you destroy or remove all business-critical information from media such as CDs and floppy disks before disposing of them. Keep in mind that simply deleting a file might not be enough to make it completely unrecoverable.
    - Make sure that all business-critical information is removed from the hard drives of any used computers before you dispose of them.
    - Store back-ups of your business-critical information either off-site or in a fire and water-proof container.

Access Control

- Use unique passwords that are not obvious (not birth dates or easily found or guessed information) and change them regularly, preferably every three months.
    - Use passwords that contain letters in both upper and lower case, numbers and special keys, and are six or more characters in length.
    - Don't write your password down, and never share it with anyone. If you do have to share it, make sure you change it as soon as possible – no matter how well you trust the person you shared it with!

Security Technology

- All computers used in your office should have anti-virus software installed, and the virus definitions must be updated at least once a week (many providers have a one-click update).
- All incoming and outgoing traffic should be scanned for viruses, as should any disk or CD that is used, even if it is from a 'trusted' source. At least once a month, and preferably every day, computers should be scanned for viruses.
- If your computers are connected to the Internet, and especially if you use a broadband connection, you must deploy a software fire-wall. This will help to prevent malicious code from entering your computer and potentially compromising the confidentiality, integrity and availability of your network. It will also help to stop your system being used to attack other systems without your knowledge. Software firewalls for use by non-professionals are readily available at a reasonable cost. Your operating system, virus control software or 'Internet Service Provider' may also offer a firewall. Consumer and popular trade magazines compare firewall functions and features of well known products, and so are a good source of information. Free shareware firewalls are available, but these usually require expert knowledge for correct use.
- System updates/patching: Complex software will always contain vulnerabilities. Criminal hackers may attempt to exploit these vulnerabilities, and the only way to protect yourself is to apply the "patches" software vendors provide. If possible, set your system

to automatically update by downloading patches when available, or at least ensure that you apply patches as quickly as possible.

- If your office has a small internal network that is connected to the Internet, you should consider deploying an 'all-in-one' hardware box that contains a firewall, anti-virus program and an intrusion detection system. This will greatly simplify your use and maintenance of essential Internet security technology.

Personnel

- Give all new employees a simple introduction to information security, and make sure that they read and understand your information security policy. Make sure they know where to find details of the information security standards and procedures relevant to their role and responsibilities.
- Ensure that employees have access only to the information assets they need to do their jobs. If they change jobs, make sure that they do not retain their access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
- Make sure that no ex-employees have access rights to your systems.
- Make sure your employees know about the common methods that can be used to compromise your system. These include e-mail messages that contain viruses and 'social engineering' ploys used by hackers to exploit employees' helpfulness to gain information that will give them access to your system. Examples of 'social engineering' include a hacker using the telephone to pose as a systems maintenance engineer or pretending to be a new employee.

Security Incident/ Response

- A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business-critical information or systems.
- Vulnerabilities in your software are an important potential source of security incidents. Vulnerabilities should be 'patched' as soon as possible after they are announced by the software vendor. Software vendors may also issue appropriate 'patches' which you can download to deal with the vulnerability.
- It is important to make your staff aware of telltale signs of security incidents. These could include:
  - strange phone requests, especially for information;
  - unusual visitors;
  - strange patterns of computer activity;
  - unusual appearance of computer screens;
  - computers taking longer than usual to perform routine tasks.
- Your staff should understand that it is always advisable to notify the right person if they observe anything that might be a telltale sign of a security incident.
- If a security incident happens, employees should know who to contact and how.
- You should have in place a plan to ensure business continuity in the event of a serious security incident. The plan should specify:
  - designated people involved in the response;
  - external contacts, including law enforcement, fire and possibly technical experts;
  - Contingency plans for foreseeable incidents such as:
    - power loss
    - natural disasters and serious accidents
    - data compromise
    - no access to premises
    - loss of essential employees
    - equipment failure.
    - Your plan should be issued to all employees and should be tested at least once a year, even if you haven't

had a security incident.

- After every incident when the plan is used, and after every test, the plan should be re-examined and updated as necessary using the lessons learned.
  - Ongoing education is vital.

Audit Controls/Due Diligence

Good information security includes knowing who has access to your system and being able to log that access. You also need to have in place a system to make sure that your security procedures are actually followed. The ability to audit and evaluate information security compliance is essential – you can’t manage what you don’t measure!

- You should audit important aspects of your security, for example, who has access to your systems and who has used what information.
- You should have a record of each one of your security procedures. For example, if your procedure says that you test your back-up generator once a week, someone should sign a record to show that this has been done. Keeping good records is essential to audit control.
- Some audit controls may be necessary for legal or regulatory purposes. Good record keeping will clearly demonstrate that you are complying with your obligations.
- An audit should ensure that the procedures you have in place are effective and relevant. It is a trigger to re-assess and re-evaluate the effectiveness of your information security standards and procedures.
- Audits are only effective if you follow through on their findings and identify and implement the steps that need to be taken. A good audit trail is not just a paper exercise. If something goes wrong, the trail should let you to see what happened and why. This will help you to keep improving the security of your business.