Risk Management for Telemedicine Providers

As a result of a member inquiry related to the delivery of medical service via telemedicine, the Risk Management department undertook a literature review on the subject. This article is a result of that review and provides a background to the practice and some salient points for practitioners to consider as part of reducing their exposure to adverse outcomes that may be associated with the delivery of a medical service via telemedicine.

Introduction

Telemedicine is a global term for any medical activity that occurs at a distance and utilises some form of telecommunications. More specifically it is sharing and transferring data and images within the practice of medicine. Other terms that have been used interchangeably for telemedicine are:

- E-health.
- Health informatics.
- Telehealth.[1]

The main objectives of telemedicine applications are to provide expertise at remote locations, access to subspecialty advice and second opinion and to provide a locum service. Telemedicine covers a range of applications including:

- Electronic medical records.
- Electronic communications including email, telephone consultations, video conferencing, web streaming (internet videoconferencing), instant messaging, decision support for rural and remote nurse practitioners and GPs.
- Specialist consultation services including teleradiology, telepathology, telepsychiatry, teledermatology.
- Websites for education or commercial purposes.

There is an absence of legislation and case law precedents relating to telemedicine in both Australia and internationally so the application of existing laws to telemedicine and the legal and ethical implications are still to be clarified.[2]

Telemedicine is constantly evolving and so practitioners should be proactive in reviewing the relevant literature and ensuring they stay up to date with clinical, technological and medico-legal developments.

Currently, there is not one comprehensive set of guidelines applicable to the Australian setting, however various policy documents and guidelines relating to telemedicine have been produced by some medical colleges and other organisations. These include the Royal Australian and New Zealand College of Psychiatrists (RANZCP) and the Royal Australian and New Zealand College of Radiologists (RANZCR).

Basic Principles for Safe Practice

The following principles form a basis for sound clinical practice where there is some element of telemedicine service delivery:

- Ethical and clinical standards and duty of care are the same for telemedicine as for face to face encounters.
- The practice of telemedicine should be the subject of rigorous ongoing assessment and evaluation of clinical effectiveness and patient satisfaction. Where possible, outcomes should be compared with standard modes of service delivery and patient feedback sought on level of satisfaction from the consultation.
- A patient's right to privacy and confidentiality of health information must be respected and maintained through compliance with Federal and State Privacy legislation.
- Where there are consultations with third parties duty of care and clinical responsibility should be clearly defined with agreement between the clinicians involved. This should include individual responsibility for defined elements of the patient's management. Always conclude the consultation by listing expected outcomes that are to be checked by the third party clinician.
- The technology that most suits the clinical requirements should be chosen (not vice versa).

- The patient has a right to fully informed consent including the benefits and limitations of the telemedicine service delivery model and alternate methods of service delivery. The patient should know that if the teleconsultation is not considered adequate then the clinician will use some other mode of treatment.

Risk Management Tip - A "face-to-face" meeting via video-link is the ideal method of establishing rapport and a satisfactory doctor-patient relationship in a teleconsultation service. Telephone and email only relationships are less likely to provide patient satisfaction.

- Appropriate infrastructure must be part of the telemedicine service to allow adequate scheduling, fault management and equipment maintenance. This will help minimise downtime allowing seamless service delivery to the patient or end-user.

Risk Management Tip - Have a policy whereby a link has to be established before the patient is brought into the consultation room. Patients will become apprehensive if the see problems with establishing the link.

- Electronic health products and services are largely unregulated so it is the responsibility of individual clinicians involved in the delivery of e-health to ensure that the delivery systems are of adequate quality.
- Providers of telemedicine services must hold the relevant qualifications and not offer advice beyond those qualifications.
- Any problem or incident identified with telemedicine delivery that results in compromised patient care should be notified through incident reporting systems. Clinicians should investigate the causes that are within their sphere of influence and where indicated, make changes to prevent their recurrence.
- The clinician and other relevant staff should receive adequate training in any new technology or software prior to its implementation in clinical practice.[3]
- Ensure that geographic separation from the patient doesn't compromise quality by having processes in place to have access to medical records and confirmation that the patient has been followed up.

Ethical, Professional and Medico-legal Issues

Privacy and Confidentiality

The legal and ethical obligations of confidentiality for telemedicine are the same as any other medical care, to ensure that any health information is only seen by those who need to see it in relation to the best interests of the patient. The following security measures will help prevent unauthorised access to confidential information.

- Use standard IT Security such as firewall control, authentication and PC timeout locking. Authentication is a system used to verify the identity of an individual and may be done through a computer login session. Also use automatic regular password changes.
- All telemedicine communications should have strong message encryption. Encryption is an electronic facility which scrambles messages so they can't be read unless the correct key is known. Password files are an example of the use of encryption. When setting up a service with a defined group of providers, ensure all Members of the service have the same encryption programs as this will assist to maintain interconnectivity and privacy.
- Telemedicine providers should have policies in place that outline specific responsibilities of technology providers, support staff and health care providers.
- Document all people who have access to confidential data and ensure that they have signed confidentiality agreements. Establish confidentiality agreements with 3rd parties - contractors or consultants who may have access to confidential information
- Use file addition and deletion security. Protect all files and folders from accidental deletion using encryption and passwords. When retiring old computer equipment use a secure file shredder program to delete confidential patient files beyond recovery. Easy to use programs with step-by-step wizards are available to encrypt and decrypt files.
- Use electronic audit trails for electronic medical records. An audit trail is a time-stamped record of the changes that users make to a record. It contains the name/identification of the user who performed the modification and typically also includes the reason for the change. An audit trail enables you to audit the system for a record of alterations, as well as to reconstruct the data at a specified point in time.
- Immediately deactivate staff passwords when they cease employment. If you have concern that termination of employment may become acrimonious, restrict or stop access to computer files for that staff member.
- Ensure that the mode of technical transmission has appropriate security. For example, don't use instant messaging, or if necessary, use Jabber which has some level of security.
- Ensure videoconferencing and teleconferencing facilities used for patient consultations are adequately sound-proofed.
- If you are upgrading a computer system and are sending hardware that contains patient information overseas for the purpose of the upgrade, you must ensure that the information remains confidential. Privacy Laws of the country you are sending the hardware to should provide at least equivalent protection as Australian laws. If you have any queries ring the Office of the Federal Privacy Commissioner on 1300 363 992.

Formation of the Doctor Patient Relationship

There are two aspects of the doctor-patient relationship that should be considered in telemedicine consultations, the formal medico-legal relationship and the informal rapport that is built between a patient and their treating clinician. It is important that the patient feels as though they can get to know the consulting clinician. A "face-to-face" video-link can be very effective in establishing a connection and is more satisfactory than email or photographs for this reason. Communication problems have been shown to escalate an incident into a claim and special care needs to be taken to ensure these are addressed in teleconsultations.

As in all interactions it is important to manage patient expectations. Set clear parameters and make sure the patient understands any limitations. You may feel that the telemedicine consultation is not progressing appropriately and need to terminate it. In this case make sure it is concluded in an appropriate manner. This may include:

- asking the patient to attend a face to face consultation;
- transferring care to a local clinician;
- transferring the patient to the local emergency department;
- rescheduling the consultation at another time; or
- where the consultation has been terminated prematurely follow-up with the patient to check that continuity of care was not compromised.

Where you have been asked for an opinion or advice on treatment regarding a patient in another doctor's care and some type of telemedicine service is used, the duty of care you have to the patient is the same as if the opinion was obtained face to face. If your opinion is subsequently implicated in a claim of negligence you are accountable for that portion relating to your opinion.

Informed consent for telemedicine consultation

As with all consent, this should be a two-way discussion and document the extent of the written and verbal explanation you provide to the patient. Where possible obtain written consent for the telemedicine service as part of the routine of obtaining consent for use of health information. Written consent should be obtained for invasive procedures or where there is potentially a higher risk such as psychotherapy sessions.

A primary consideration when determining the suitability of a videoconference consultation is whether the patient is willing and able to sit in front of a camera and communicate. Other specific issues to include in telemedicine consent are:

- Clinician's name and qualifications.
- That the consultation will be performed at a distance via some type of telecommunications.
- A warning to the patient.
- That lack of opportunity to physically examine the patient may increase the risk of misdiagnosis or missed diagnosis.
- That technical limitations of the mode of consultation may effect accuracy eg in diagnostic imaging applications where mode of transmission may affect image quality.
- That where the teleconsultation is not considered adequate by the clinician then another mode of treating the patient will be put into effect.
- The nature and potential risks and consequence of risks.
- Any risks to privacy and confidentiality of clinical information.
- Alternate options for treatment/management/consultation.
- To obtain the consent of the patient for any additional people who may be in attendance during the telemedicine consultation.
- To obtain written informed consent from the patient if you wish to record (video and/or audio) any part of a consultation.

Both the clinician and the patient should be able to terminate the consultation at any time if it is determined that adequate information cannot be obtained or the mode of consultation is not appropriate.

Access to Services

Telemedicine has the potential for providing fairer access to higher quality services for patients, particularly in rural and remote locations. With appropriate use of centres of excellence it provides the opportunity for patients to access safer care nearer to home and in some cases with reduced waiting times. Clinicians should be aware of telemedicine services that may benefit their patients or where their contribution to such services will improve patient care.

State and Territory Medical Boards agreed that "any contact that results in written or documented medical opinion (phone, email, and internet) and that affects diagnosis or treatment of patient constitutes practice of medicine. Telemedicine was to be regulated by the medical board in the state the patient resided. To operate lawfully, the medical practitioner must be registered in that State".[4] (Medical Forum September 2004)

Documentation

In addition to usual documentation requirements, clinicians are responsible for ensuring that documentation for each telemedicine session includes:

- Mode of service delivery.
- Sites that were linked.
- Attendees at the session including names of healthcare professionals and others present.
- Any technical difficulties that occurred that impacted on the clinician's ability to discharge their duty of care.
- Where a clinician is consulted in a consultation liaison model then they should document a detailed assessment, any treatment recommendations and responsibilities among the team for each element of the patient's management.

Standard of Care

Where a General Practitioner (GP) is consulting with a specialist in the management and/or treatment of a patient then the GP must exercise the requisite skill in providing that treatment. Recent tort law reforms in some States (NSW, Victoria, Queensland and WA) have reverted the standard of care by which doctors will be judged to that which is widely accepted by peer professional opinion as competent professional practice (the modified Bolam Principle). In circumstances where the GP undertakes to perform a specialist procedure (at the direction of a specialist through a telemedicine consultation), the GP may be judged by a similar standard of care as that of the supervising specialist. The patient, having made contact with a specialist, will anticipate a specialist level of expertise. In this situation it is essential that the patient is warned and understands that it is a GP performing a specialist procedure.

The GP must inform the patient of all the material risks including the names of doctors who are specialists in performing the specific procedure and document this discussion. The patient should be given the option of going to these specialists if it is practicable although it is acknowledged that within rural and remote situations the cost-benefit of transporting patients will exclude this option in many cases.

The Australian Medical Council has determined that the standard of care that applies when consulting a patient by telemedicine is that of the patient's home state or territory even if the clinician is geographically located elsewhere.[5] Clinicians' should be aware that this differs from some other countries where the relevant standard of care is that of the site of the clinicians practice.

Insurance Matters

Generally speaking MDA National Insurance Professional Indemnity Insurance Policy (PIIP) covers indemnity claims arising from the provision of telemedicine services, however, the following issues should be noted and if there is any doubt as to coverage this should be confirmed with your insurer.

If you are in a practice that utilises the services of clinicians who provide the service from a base in another country, such as a teleradiology service, you should be aware of any legal issues pertaining to their status in the event of a claim arising from the services they provide. Be aware that the law that applies is generally the law of the country where the cause of action arose but what this means may be subject to different interpretations in different jurisdictions. For example, where the doctor providing a third party consultancy or the patient resides in another country, they may start litigation in that country rather than in Australia. Members should check if their professional indemnity insurance policy has any restrictions on:

- the jurisdiction you are permitted to practice in, and
- the jurisdiction that claims can be first made.

For instance, the 2005/06 MDA National Insurance PIIP excludes claims arising out of acts, errors or omissions which occur within the USA or Canada. It also will not respond to claims where the proceedings are commenced in the USA or Canada.

Models of Service Delivery

Radiology

The use of offshore personnel for interpretation of locally acquired radiological images is being increasingly used in Australia. Some Australian based radiologists are also providing "nighthawk" reporting services to US and Europe. The RANZCR policy on teleradiology recommends that radiologists providing these services be licensed and have medical malpractice insurance in both the jurisdiction where the images were gathered and transmitted from and the jurisdiction where they provide the service.[6]

The policy also provides guidance on the "professional supervision" of the examination (request cards, patient information, tailoring the examination). Practitioners should ensure that the following points are clarified before providing any remote teleradiology service:

- Does your insurer cover you for the services you provide for patients resident overseas (please note that the MDA National Insurance PIIP does not cover for services provided in USA and Canada)?
- Do you have medical registration in the jurisdiction in which you are providing services?
- Are there any additional credentialing requirements for that jurisdiction?
- Does your practice have a contract that outlines obligations, minimum levels of hardware quality and indemnity requirements with the organisation delivering/receiving the services?
- When providing reports for images acquired elsewhere, do local radiologists check interpretations, sign and submit final reports?

Consultation Liaison

The consultation liaison model involves local health care professionals providing the primary management of the patient's care but a specialist medical practitioner assessing the patient and giving guidance on diagnosis and appropriate treatment. In this model the patient, the local health practitioners and the specialist may participate in a joint video consultation. Subsequently the specialist may assist with further queries about the patient but does not necessarily have active involvement in their ongoing care. One of the key issues that may increase a doctor's risk of a claim is that of abandonment. The consulting doctor needs to ensure that arrangements have been made and carried out to provide ongoing care and that these arrangements have been communicated to the patient.

Key principles for safe practice with this model include:

- Clear agreement regarding responsibility for treatment and follow-up.
- Concluding the consultation with the specialist listing expected outcomes that are to be checked by the local clinician. If these outcomes are not achieved then a further consultation needs to be undertaken.
- The specialist dictating a letter back to the local/referring clinician outlining the features which were taken in the history, the clinical findings as seen from the specialist's end and the next steps expected.
- Each clinician being held accountable for that part of the management in which they participate.

Outpatient/Primary Care Management

If the clinician providing the telemedicine service is assuming full responsibility for management of the patient's care then the relationship and accountabilities are the same for a face-to face model of care. Special consideration should be given to managing issues such as physical examination and monitoring compliance with treatment. Where the telemedicine encounter is for the purpose of providing treatment, due consideration should be given to any possible complications of the treatment and steps taken to ensure that contingency plans for emergency care are in place.

Where a psychiatrist conducts a psychotherapy session from a distance they need to ensure that the patient has adequate support on site including someone who can drive them to the therapist or a hospital if the need arises.[7]

Electronic Medical Records

Increasing numbers of medical practices and hospitals have now changed or are preparing to change to an electronic medical record. These may be paperless or a combination of paper and electronic. The following issues should be considered when implementing or reviewing an electronic records system:

- Ensure the software system is fit for the purpose.
- Make sure you have adequate technical support and that contingency plans and support contact numbers are accessible to staff. Where possible have a contract with your technical support group that specifies minimum acceptable response time when a critical failure occurs.
- Ensure that you have on and off site backups of all files. Record and regularly verify backup procedures.
- Have security measures in place and ensure privacy of personal and health information.
- Where there are both paper and electronic records, have a process in place that flags the existence and location of other format (eg hardcopy) records.
- Have facilities available that allow access to electronic records if requested by the patient. If someone other than the patient requests access to a medical record ensure that you have written authority from the patient first.

Email

Clinicians should discuss the ramifications of communicating electronically with patients and obtain documented informed consent before using email. The security issues discussed previously also relate to email.[8] Other issues to be considered when using email:

- Clinicians should not provide an email consultation to an unknown patient.
- Confirm with the patient the email address to be used for communication about their health care.

Risk Management Tip - only send information as a reply to an email sent to you by the patient.

- Any email communication with patients should be retained with the patient's record.
- Use an automatic return receipt to check an email has been received. Ask patients to acknowledge that they have received and read the email. Flag as "outstanding", emails where acknowledgement has not been received.
- Don't use email for communication of urgent information. Include a reminder at the bottom of your email to the patient that it is important that they use the telephone or face to face communication if the matter is urgent.
- Email doesn't replace face to face communication. Only use it for clinical advice if you already know and have a relationship with the patient.
- Use message encryption. Some State and Territory Health Departments only authorise emails containing information about patients between addresses on Health Departmental email servers.[9]

Instant Messaging

Instant messaging (MSN, ICQ etc) used for chat rooms and internet video conferencing is generally not secure and so is not appropriate for use for patient consultations. One exception is the Jabber protocol which includes a level of authentication and security.

Some health services are using mobile phone text messaging for monitoring chronic diseases such as diabetes. Text messages are not secure and so should not be used as a method for communication of health information.

Internet as an Information Resource

The internet is a useful resource to help stay up to date. Be aware that information on the internet is not necessarily validated. Only use those sites that are backed by organisations that have rigorous methods for validating website content. Government, professional organisations, journals and university sites will have a process to check website content. If in doubt use the same critical appraisal criteria you would use on any written information.

Most people are now very familiar with using the internet to access information. Health related websites are becoming more and more popular. While you can't control your patient's access to these information sources, you can identify websites that have reliable consumer information for use as a reference by your patients. It may be useful to construct a list of reliable websites with information relevant to your specialty.

Establishing Your own Website

If you wish to set up a website of your own, either as an information site for your patients or to advertise your medical practice, there are issues you need to consider. People who use a health related website should be provided with information that allows them to judge if the website is credible and trustworthy. There are a number of issues that should be addressed when developing your own website. Some of the key points are:

- When making claims or representations ensure that you are not in breach of the Trade Practices Act eg for misleading and deceptive conduct. It is suggested that you seek independent legal advice about Trade Practice requirements before posting a website in the public domain.
- Make sure the intent of the website is clear on entry to the site. State whether it aims to promote your practice or to provide clinical information to the general or healthcare community.
- State clearly who owns the site or who has a significant financial interest in the site including any sponsorship of the site.
- Ensure information is current and factual and have a policy for regular revision and updating of all information on the website. Display the last updated date on all pages.
- Do not include any personal information on your business website.
- Don't provide links to other websites unless they are reliable and updated regularly.
- Use appropriate disclaimers and warnings particularly when providing clinical information.
- Clearly state any copyright ownership of specific content and ensure it appears on printed copies. Source any specific content in the same manner as a peer reviewed journal.
- Where possible, provide documents in downloadable PDF format. Include a large file warning for documents larger than 500kb.
- Do not set up a chat room on your site if you don't have a secure password protected area.
- The use of websites for the purpose of advertising is not considered to be appropriate by many Medical Boards and Members should ensure that they comply with the regulations of the respective State and Territory Medical Boards in this matter. If you do have advertising on your site ensure it is easily distinguished from content.[10]
- If using a "cookie" on a website to permit tracking of personal information, the user should be able to opt out of this function at any time. Cookies are a technology that enables Web sites to store small bits of information on your hard drive, and then ask for that information back at a later time. They are very small (maximum size 4 kb), non-executable files (not programs).
- Make sure your privacy policy is updated to cover the operation of your website and is published accessibly on the site.

There are credible organisations that can assist in setting up a website. If you or someone in your practice has Membership with the Australian Association of Practice Managers (AAPM) they will set up a personalised website for your practice as part of membership benefits.[11] For more detailed guidelines on Medical websites see American Medical Association Guidelines for Medical Information Web Sites.[12]

Clearly telemedicine has a valid and growing following amongst medical practitioners. However, apart from practical issues associated with the setting up, training and use of the equipment, there are some inherent challenges that must be addressed before providing a medical service using this technology. These include privacy and confidentiality, who clinical responsibility and duty of care sits with, training of appropriate staff, consent issues, and an awareness of any restrictions related to the practitioners' medical indemnity insurance in particular, international jurisdiction.

There is no doubt that the use of this technology to provide medical services, particularly to remote areas, has a place and as the use of these services becomes more popular the legal and ethical implications or this practice will become clearer.

Risk Management Services

References

[1] Wootton R. *Telemedicine* BMJ 2001, 323; 557-560.

[2] White P. *Legal Issues in teleradiology - distant thoughts!* Br J Radiol 2002, 75; 201-206.

[3] *e-health Code of ethics* http://www.ihealthcoalition.com

[4] Medical Board of Western Australia Policy: *Telemedicine*. 2003

[5] Medical Practitioners Board of Victoria. *Statement on Telemedicine*. http://medicalboardvic.org.au/content.php?sec=62

[6] *RANZCR Position on Teleradiology 2001* http://www.ranzcr.edu.au/about/guidelinesandpolicies/index.cfm

[7] The Royal Australian and New Zealand College of Psychiatrists. *Position Statement #44 Telepsychiatry* http://www.ranzcp.org/pdffiles/posstate/ps44.pdf

[8] Car J, Sheikh A (2004) *Email consultations in health care: 2 - acceptability and safe application* BMJ Vol 329: p439-442

[9] A. R. Spielberg (1998) *Sociohistorical, Legal, and Ethical Implications of E-mail for the Patient-Physician Relationship* JAMA. 1998; 280: p1353-1359

[10] PIAA. *Telemedicine - A Medical Liability White Paper*

[11] *AAPM* http://www.aapm.org.au/

[12] American Medical Association (2000) *Guidelines for Medical Information Web Sites* http://jama.ama-assn.org/cgi/reprint/283/12/