Practice Managers' **Update 2013**

Overview

This update provides a "snapshot" of the emerging and perennial medico-legal issues in practice management today. Specifically written for Practice Managers and practice staff, this publication aims to provoke thought, highlight common medico-legal risks and support quality medical practice management.

This edition covers:

- marketing your practice in the digital age and the medico-legal considerations
- medico-legal considerations of advertising and email use
- security of electronic records
- Personally Controlled Electronic Health Records (PCEHR) program and the role of a Responsible Officer
- telehealth.

Please contact our Medico-legal Advisory Service about any specific cases or concerns on 1800 011 255 or advice@mdanational.com.au.

If you have any feedback, comments or suggestions for future editions, email us at specialtyupdate@mdanational.com.au.

Marketing Your Practice Effectively in the Digital Age

Guest writer – Riwka Hagen, Practice Manager, Accreditation Surveyor and Practice Management Consultant.

Medical practices are increasingly looking to online media to market their services, engage and communicate with patients and provide a platform for interaction and delivery of health-related resources and information.

With the ability to engage using a wide variety of online communication tools such as customised websites, social media, video sharing, blogs and mobile technologies, strategies need to be in place to ensure that as practices progress from simple information sharing to increased levels of engagement, activity is managed effectively and that the potential risks in doing so are minimised.

Websites

Many practices now have an online presence, ranging from simple single page websites providing basic information to more elaborate designs providing additional detail and promotional material.

Below are some basic considerations when developing your practice website:

- Consider free website building tools such as Wix or Webs to get started.
- Ensure that information is updated, current and accurate. Out-of-date information sends a poor message to patients.
- Ensure language, spelling and grammar are professional.
- Content must be consistent with best practice and evidence-based.
- The use of widgets and content syndication such as RSS embedded to your website from reputable health-related websites will provide up-to-date content that requires no active input. Websites such as betterhealth.vic.gov.au freely provide the tools to enable content sharing. However, it is important to be mindful of linking to or getting content from external websites as you cannot always guarantee its accuracy.
- Websites are not only useful for patient information, but provide prospective employees a snapshot of your practice – use this advantage to attract the right candidates.

Your practice website – medico-legal considerations

It is important to be familiar with and adhere to the Medical Board of Australia's *Guidelines for advertising of regulated health services*. The relevant section of the National Law states that health services must **NOT** be advertised in a way that:

- is false, misleading or deceptive or is likely to be misleading or deceptive
- offers a gift, discount, or other inducement to attract a person to use the service or business, unless it is also states the terms and conditions of the offer
- includes testimonials or purported testimonials about a service or a business
- directly or indirectly encourages the indiscriminate or unnecessary use of regulated health services i.e. encourages inappropriate, unnecessary or excessive use of the health service; for example to "achieve the look you want".

Be especially careful of using "before and after photos" as they must be:

- of a real patient and you must have the patient's consent to use them
- as similar as possible in the set up e.g. the same lighting, background and distance from camera
- have the procedure as the only change for the person being photographed.

Read the Medical Board of Australia's *Guidelines for advertising of regulated health services* in full at **medicalboard.gov.au/Codes-Guidelines-Policies.aspx**. It is also advisable to check if the College which your practice is associated with provides website standards or guidelines that you also must comply with.

Additionally, the Therapeutic Goods Administration (TGA) also places restrictions on advertising certain medications, for example, names of drugs such as Botox and fillers cannot be used.

Always seek advice about any medico-legal concerns associated with your website from MDA National.

Get educated about the risks and consequences of social media before you implement any strategies for your practice.

Social media

Embarking on a social media presence such as Facebook or Twitter can allow practices to engage on a new level, especially with younger patients who are most fluent with these platforms. Use of such media allows for far more direct engagement and as a result, also requires a different level of interaction and involvement. A Facebook page is easy to create but requires constant monitoring to prevent stagnation and to ensure interaction remains appropriate and professional at all times.

There are four key attributes of social media channels that are believed to make them highly effective as health communication tools.

- Personalisation – content tailored to individual needs.
- Presentation – timely and relevant content accessible in multiple formats and contexts.
- Participation – partners and the public who contribute content in meaningful ways.
- Viral effect – many social media channels facilitate social engagement, viral exchange of information and trust.

One of the pitfalls of social media is the potential for negative publicity to occur quickly when a disgruntled patient decides to air their grievances, on for example, the practice's Facebook page. The fall-out from such events can be devastating for the practice and difficult to control. It is recommended that engagement with the public via Facebook or Twitter remains generic in nature – provision of health articles of interest and broad outline of services offered – and that direct interaction with the public is restricted to general comments only. A public reminder that the Facebook page should not be used for asking questions that relate to individual health concerns or service issues will set the scene for appropriate interaction. Posts by the public that are deemed to breach privacy rules should be removed immediately and responded to privately.

Although a social media presence has the capability to vastly improve communication with patients and clients, it clearly requires far more active management and therefore should not be undertaken unless this vigilance can be maintained. Professional standards must apply in the creation and management of social media.

Questions or comments?
Email us at
specialtyupdate@mdanational.com.au.

Social media – hints and tips

- Maintain confidentiality and privacy laws, before making a post. If putting up a picture, ensure that the patient is completely de-identified or that you have their consent.
- Present information in an unbiased, evidence-based context and do not make unsubstantiated claims.
- Do not use your own Facebook/ Twitter account to market the practice – have very separate personal and professional online identities.
- Facebook – ensure relevant privacy settings, and only allow a designated page administrator to post content. Settings can also be modified so that before a post is added to your page the page administrator can review it.
- Post or update regularly to improve your search engine ranking (search results on search engines such as Google).
- Get educated about the risks and consequences of social media before you implement any strategies for your practice.
- If you receive a complaint or negative feedback through your social media channels, or you have any other medico-legal concerns relating to social media contact MDA National to obtain advice on how to deal with it.

Familiarise yourself with and adhere to:

- The Medical Board of Australia's *Guidelines for advertising of regulated heath services* available at: **medicalboard.gov.au/Codes-Guidelines-Policies.aspx**
- The Australian Medical Association, New Zealand Medical Association, New Zealand Medical Students' Association and Australian Medical Students' Association *Social Media and the Medical Profession. A Guide to Online Professionalism for Medical Practitioners and Medical Students*. Available at **ama.com.au/social-media-and-medical-profession**.

Summary points

- Assess time, cost and expertise before undertaking online activities.
- Ensure you have appropriate technology and support.
- Be aware of the pitfalls of online presence.
- Adhere to the Medical Board of Australia's *Guidelines for advertising of regulated health services*, relevant College and Practice Accreditation Standards requirements.
- Ensure patient privacy and confidentiality are maintained at all times.
- Keep online information updated and current at all times.
- Use online tools not only to engage with patients, but to provide a marketing advantage to attract service providers.
- Be careful of other websites that the practice website is linked to as it is difficult to guarantee the accuracy of content of those sites.

Always seek advice about any medico-legal concerns in relation to marketing your practice from MDA National.

Riwka Hagen has over 18 years' experience in practice management. She is a Practice Manager, Accreditation Surveyor with AGPAL and provides medical practice advisory, consultancy and training services through *Medical Business Services*.

Telehealth

Telehealth covers a wide variety of delivery methods and is becoming more common across the healthcare spectrum. Telehealth consultations are not always appropriate and it is up to the medical practitioner to determine its suitability.

The following tips may assist if your practice uses or is considering implementing telehealth:

- Choose or ensure existing equipment such as computers are suitable for telehealth. In order to claim under the Medicare Benefits Schedule for a telehealth consultation, audio and visual capability is required.[1]
- Choose a system that maximises privacy and security of information before, during and after the telehealth consultation. Skype™ is not recommended due to security concerns.
- Ensure equipment is well maintained; for instance, regularly reviewed by a reputable information technology provider and ensure current antivirus/antimalware and firewalls are in place.
- Consider using a computer for visual purposes but a telephone line for audio. This helps with visual quality and enhances privacy/security.
- Check that the patient's record has a signed written consent prior to the initial telehealth consultation. It is essential that the patient consents to a telehealth consultation before the consultation commences.

Patient information pack

A patient information pack containing a brochure and consent form which can be sent out or given to the patient prior to a consultation is useful to inform the patient.

The brochure could cover:

- What the telehealth consultation is and its benefits and restrictions.
- What is involved and how to prepare, particularly if photographs need to be taken.
- The importance of visual and audio privacy at the patient's end and how to address issues.
- The associated costs.
- That consent to take part in telehealth consultations can be withdrawn at any time.
- The requirement that recording of consultations is not accepted, even by the patient. The doctor may, with the express consent of the patient, record a portion of the consult e.g. if the patient has a wound or gait/movement concerns.

Sample consent forms can be found at:

Queensland Health at health.qld.gov.au/telehealth/docs/pat_consent_form.pdf.

1 *Medicare Australia. Telehealth Frequently Asked Questions.*

Personally Controlled Electronic Health Records Program

The Role of a Responsible Officer

For any medical practice that wants to participate in Personally Controlled Electronic Health Records (PCEHR) a raft of practice based roles have been created to facilitate the program. However, for Practice Managers, there are some key aspects to be aware of.

What is a Responsible Officer?

The practice is required to appoint a person to be responsible for interactions between the practice and the Systems Operator (the Department of Health and Ageing) in the PCEHR system.

The role of the Responsible Officer is to:[1]

- Register the practice to obtain a Healthcare Provider Identifier – Organisation number.
- Register the practice to participate in the PCEHR program.
- Be accountable for the practice's interactions with the PCEHR program.
- Be accountable for and oversee the setting of access levels for different levels of staff likely to need access to the system including healthcare providers and administrative staff.
- Be accountable for staff who will conduct administrative tasks associated with the PCEHR or perform those tasks in a stand-alone practice.
- Appoint a staff member to be the Organisation Maintenance Officer and link each practice in a network of practices with the PCEHR system or alternatively, perform the duties of the practices' Maintenance Officer in a stand-alone practice.

Further information about the practice based roles required for PCEHR and, in particular, the Responsible Officer can be accessed from the Department of Health and Ageing eHealth website: **publiclearning.ehealth.gov.au/hcp/how-do-we-get-ready/getting-your-practice-ready/**.

What are the risks for Practice Managers?

As the Practice Manager and Responsible Officer you need to be aware of the risks associated with:

- inappropriate access to the PCEHR system if security levels are not set appropriately
- failure to have adequate systems in place to monitor breaches of the system and therefore the agreement with the Department of Health and Ageing
- lack of appropriate staff training and supervision
- poorly maintained information technology systems which can result in unauthorised external access (hacking)
- lack of personal awareness of the ramifications associated with being a Responsible Officer for a network of practices.

How to minimise the risks?

To minimise the risks you should:

- Fully investigate the expectations associated with being the Responsible Officer before accepting the role, including obtaining advice from MDA National.
- If you are not the designated Responsible Officer you should not perform any of the functions of the Responsible Officer. The Responsible Officer must undertake these tasks and not delegate them.
- Conduct a review of information technology systems, policy and procedures and staff training prior to registration with the PCEHR system.
- Implement changes identified in the review.

1 *Medicare Responsible Officer User Guide*. Available at: medicareaustralia.gov.au/provider/health-identifier/files/his-responsible-officer-user-guide.pdf.

Bonus Material

Is Your Practice Invisible?

Although not seen as a traditional avenue of marketing, medical practices are becoming increasingly aware of the importance of a powerful online presence. Research now confirms that nine out of ten people use an online search to find a local business.[1]

Tristan Bond from Healthcare Business Coaching and author of *7 Steps to Unlimited Patients: How to Build a Multi-Million Dollar Practice the Easy Way* outlines five simple tips for developing and maintaining a successful practice website.

To read the article in full visit **defenceupdate.mdanational.com.au/pmupdatebonus.**

1 *WebVisible with Neilson Rating. Why search matters to local businesses. Available at: c.ymcdn.com/sites/www.sempo.org/resource/resmgr/Docs/why_search_matters_to_local.pdf.*

Security of Electronic Records

As a Practice Manager for a busy practice, you sit down at the practice computer one morning, and an alert flashes up on the screen – your computer has been hacked and your patient records encrypted. A ransom of several thousand dollars is demanded before the hackers will decrypt your records to enable access.

Cyber-crime is not new but targeting health practices is an emerging risk. After the hacking and ransom of a Gold Coast medical centre's records in December 2012, this issue became known to doctors and public alike. Media sources stated that there had been 11 similar incidents in Queensland alone during 2012.[1]

Practice Manager's role in prevention:

There are simple but preventative actions that can be taken to minimise the risk of data loss:[2]

- maintain appropriate security measures (including firewall/antivirus software)
- have an adequate computer backup system
- ensure appropriate technical support
- formulate a disaster recovery/business continuity plan (in a worst case scenario, what will you do to ensure you are able to maintain continuity of care and recover your lost data and records).

An excellent resource is the Royal Australian College of General Practitioner's (RACGP) *Computer and Information Standards* and although general practice focused, these standards are easily applicable to any medical practice.

Adequate, reliable and timely database backup is critical. How frequently you back up your records will limit the amount of data that cannot be recovered. Backups need to be securely stored off-site and regularly tested for integrity.

Dealing with a privacy breach following a hacking incident

In the event that practice records are hacked and records accessed by the intruder, this will constitute a breach of privacy. From March 2014 with changes to the *Privacy Act 1988* (Cth), significant civil penalties may apply for these kinds of breaches.[3] Therefore, it is important that as a Practice Manager you should:

- instigate the practice business continuity/disaster recovery plan immediately
- contact Medicare, and other agencies involved in patient care
- contact the practice indemnity insurer and seek further assistance, including when and how to contact patients.

The Office of the Australian Information Commissioner (OAIC) has a helpful guide discussing how such a data breach can be addressed.[4]

The OAIC considers there are four steps to respond to a major data and privacy breach:[5]

(1) containment and assessment
(2) evaluation of risks associated with the breach
(3) notification (not mandatory at present but this is being considered and may result in an investigation by the OAIC)
(4) prevention.

Data loss and privacy breaches are serious matters. Irrespective of the cause, they can result in significant disruption to the practice and result in claims, complaints and investigations. The key to limiting the impact is prevention.

Recovery

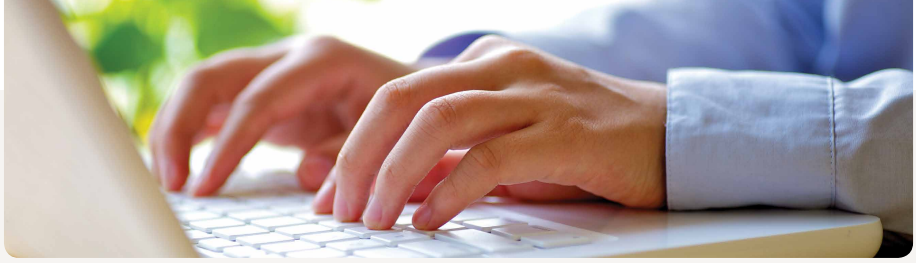
In the event of data loss, it is critical to know where your most recent backup is located. Loss of records cover is provided under the MDA National Insurance's Practice Indemnity Policy and Professional Indemnity Insurance Policy, and includes indemnification for reasonable costs and expenses incurred in recovering documents, subject to the terms and conditions of the policies.

For more information about our Practice Indemnity Policy including why a practice needs its own indemnity policy see the "Snapshot" section on the back page of this update.

1 goldcoast.com.au/article/2012/12/10/443366_gold-coast-news.html.
2 racgp.org.au/your-practice/standards/ciss/.
3 Federal Court proceedings brought by the Privacy Commissioner can award civil penalties of up to $340,000 for serious or repeated breaches of the Privacy Act. These changes will commence on 12 March 2014 following changes to the *Privacy Act 1988* (Cth) by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
4 oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html.
5 oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

Adequate, reliable and timely database backup is critical. How frequently you back up your records will limit the amount of data that cannot be recovered.

Medico-legal
CASE STUDY



This case study outlines the importance of understanding the guidelines associated with advertising medical practices and how to avoid breaching privacy and confidentiality with the use of email.

A practice decides that it is time to "get online". The practitioners assign the responsibility of the practice website to the Practice Manager with some support from one of the doctors, Dr A.

The Practice Manager attends a marketing workshop. Following the workshop, she puts together a plan for developing a website and a Facebook page. She has a brief meeting with Dr A to discuss her ideas. Dr A vaguely mentions reading about advertising guidelines for medical practices but isn't sure if they apply to all specialities. He gives the Practice Manager the go ahead to employ an advertising agency to develop the website and Facebook page as per her plans.

The website and Facebook page are launched and a 10% discount on procedures is offered for a month. The Practice Manager asks the Administration Assistant to send an email to the practice's patients to "like" the practice's Facebook page and receive a discount on their next treatment. The email is successfully delivered but unfortunately includes all the recipients' email addresses within the message.

A furious patient contacts the practice the next day saying the practice has breached her confidentiality. Another patient complained that she received an email advertising health supplements referencing the email from the practice as the source of contact.

The Practice Principal asks the Practice Manager to explain what went wrong.

Medico-legal issues

- Inappropriate delegation of responsibility to the Practice Manager.
- Inadequate supervision of staff.
- Inappropriate advertising.
- Breach of privacy and confidentiality.

Minimising the risks with advertising

Practice Managers are often heavily involved in the marketing and advertising of the practice. However it is important to remember the final decisions and sign off lie with the medical practitioners –The Medical Board of Australia's *Guidelines for Advertising of regulated health services* (the Guidelines) strictly state this responsibility is with medical practitioners and it cannot be delegated to another party or to an agency.[1]

As the Practice Manager you should however be familiar with what can and can't appear on a practice website and other advertising material.

These are:[1]

- Practitioners' qualifications can be listed, but particular care needs to be taken to avoid the use of statements such as the "best surgeon in town".
- Testimonials are prohibited.
- Offers that are likely to encourage indiscriminate or overuse of medical services cannot be used.
- There are specific requirements for the use of before and after photographs.
- Where a surgical or invasive procedure is advertised directly to the public, the advertisement must include a clearly visible warning as specified in the Guidelines.

A registered health practitioner, or a business providing a regulated health service, whose advertising breaches the National Law, may be liable for a $5,000 penalty (for an individual) or $10,000 (for a body corporate). The relevant National Board may also decide to manage a practitioner's persistent breach of the National Law through its conduct, health or performance pathways, which may include placing restrictions on an individual's registration and their ability to practise.

The Therapeutic Goods Administration[2] also governs medical advertising and prevents the naming of particular medications such as dermal fillers. Consumer protection laws also cover advertising to prevent misleading or deceptive advertisements.[3]

Privacy and confidentiality and lack of staff supervision

Breaching patient privacy and confidentiality can have significant impact for Practice Managers. It is possible that as an individual, the Practice Manager could be held accountable and receive a fine of up to $300,000 if found guilty of a serious breach.[4]

Therefore, as a Practice Manager you should ensure that:

- Staff receive adequate training as part of their induction on confidentiality and privacy.
- Staff sign confidentiality agreements on commencement.

Breaching patient privacy and confidentiality can have significant impact for Practice Managers.

- Regular staff training is conducted.
- The practice has an up-to-date privacy policy and this is reviewed regularly.
- The practice complies with relevant College or speciality organisation guidelines regarding privacy.

General risk management actions

Apart from the actions mentioned above, the following can also minimise the risks associated with emails and advertising, protecting practice staff, including the Practice Manager:

Advertising

- Do not accept sole responsibility for the advertising of the practice. All advertising must be signed off by the practice principal before it is put in place.
- Familiarise yourself with and adhere to the Medical Board of Australia's: *Guidelines for advertising of regulated health services*, available at: **medicalboard.gov.au/Codes-Guidelines-Policies.aspx** and *AHPRA's Frequently Asked Questions; Advertising*, available at **ahpra.gov.au/Legislation-and-Publications/AHPRA-FAQ-and-Fact-Sheets/advertising-faq.aspx**.
- Where you are asked to liaise with an external agency, ensure the agency knows what your role in the process is.
- If before and after photographs are used, ensure proper written consent is obtained from the patient and is kept on the patient file. The patient's identity should never be included with the patient's photographs.

Use of emails

- Limit the use of email between the practice and patients to administrative matters only, or decline to email patients.
- Use signs in the reception area to alert patients to the practice policy on email use.
- If email is used, ensure you have the patient's consent to being contacted via email.
- Always address patient complaints about breach of privacy and confidentiality quickly.
- Regularly check and update patient contact details including email.

You can also contact MDA National for assistance.

Conclusion

The Practice Managers' liability for the breach of advertising guidelines may be covered under the Practice Indemnity Policy but clarification would be required to ensure this is the case. More importantly, there could be other ramifications such as dismissal.

The actions of the Administration Assistant and the Practice Manager in sending out an email that breaches confidentiality and privacy are more likely to be covered under the Practice Indemnity Policy as an unintentional breach of privacy – contact MDA National to discuss your specific situation.

For information about our Practice Indemnity Policy including why a practice needs its own indemnity policy see the back page or contact us for our Practice Health Check brochure to find out more.

1 Medical Board of Australia, *Guidelines for advertising of regulated medical services*. Available at: medicalboard.gov.au/Codes-Guidelines-Policies.aspx.
2 tga.gov.au/industry/advertising-schedule4-substances.htm.
3 *Competition and Consumer Act 2010* (Cth).
4 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

Workshops

Keys to a Healthy Practice Workshop
Open the door to excellence in your practice

This 90-minute, interactive, small group workshop explores key factors of workplace excellence and what makes the workplace special for staff and how to successfully move forward with practice improvement initiatives. It is ideal for all members of the practice team.

Online Communication for Medical Professionals

Embrace social media and other communication technologies in ways that benefit health care while protecting your patients and your practice. This two-hour, highly interactive workshop explores how to maintain privacy and professionalism when using online communication methods and is ideal for all practice staff and doctors.

Interested in hosting any of the above workshops at your practice? Email events@mdanational.com.au today.

Snapshot

Is your practice protected?

At the heart of your medical practice is a team of clinical healthcare professionals and practice staff that, if not protected, can create significant risks to the practice, its staff and its owners.

Practices may need their own **Practice Indemnity Policy** to:

- protect the practice entity and its employees against civil liability claims which arise from the provision of healthcare services
- cover the practice from acts or omissions of practice employees acting outside the supervision of a medical practitioner
- protect the entity against a range of professional investigations, complaints or proceedings such as privacy breaches, ACCC investigations, mandatory reporting and defamation
- ensure consistent coverage for all practice employees under one policy and avoid unnecessary gaps between different policies
- complement medical practitioners' individual professional indemnity policy
- protect the reputation of the practice and its employees.

MDA National Insurance's Practice Indemnity Policy provides a broad cover based on our experience and knowledge of practice risks.

Contact us on 1800 011 255 or peaceofmind@mdanational.com.au for more information.

Freecall: 1800 011 255
Member Services Fax: 1300 011 244
Email: peaceofmind@mdanational.com.au
Web: mdanational.com.au

MDA National
Support Protect Promote

Adelaide
Unit 7
161 Ward Street
North Adelaide SA 5006
Ph: (08) 7129 4500
Fax: (08) 7129 4520

Brisbane
Level 8
87 Wickham Terrace
Spring Hill QLD 4000
Ph: (07) 3120 1800
Fax: (07) 3839 7822

Hobart
GPO Box 828
Hobart TAS 7001
Ph: 1800 011 255
Fax: 1300 011 244

Melbourne
Level 3
100 Dorcas Street
Southbank VIC 3006
Ph: (03) 9915 1700
Fax: (03) 9690 6272

Perth
Level 3
88 Colin Street
West Perth WA 6005
Ph: (08) 6461 3400
Fax: (08) 9415 1492

Sydney
Level 5, AMA House,
69 Christie Street
St Leonards NSW 2065
Ph: (02) 9023 3300
Fax: (02) 9460 8344