Telehealth & Practice Risks Guide

Reading time:
Pamela Ferrada
Last Modified on 06/05/2024 9:03 pm AEST

Professional indemnity – matching your risk exposure to the right classification

It is a mandatory registration requirement of the Medical Board of Australia, that as a healthcare practitioner who undertakes any form of clinical practice, **you must have professional indemnity insurance or some alternative form of indemnity cover**. Your initial and yearly renewal of your registration will ask you to declare that you are covered for all aspects of your practice for the entire period of registration.

How to mitigate your clinico-legal risk

- Once you start practicing privately, you must notify your medical defence organisation to ensure the right indemnity cover is in place and commensurate with your new risk exposure.
- Regardless of your career stage, it is critical that you are assessed against the right professional indemnity classification. Failure to do so may jeopardise your indemnity cover and level of protection against claims, complaints and/or investigations from patients, AHPRA, the Boards or any other regulatory agent. There are usually options for non-procedural and procedural work and various billings bands as well as endorsements for cosmetic procedures. Make sure you are in the right professional indemnity category.
- If you work at a public hospital and or are an employee, your employer is vicariously liable for your omissions or negligence, if it falls within the scope of your work at the institution. Always get written approval. While this meets the AHPRA indemnity requirement, you may obtain additional cover by joining a medical defence organisation to provide you with back up cover for the provision of any healthcare that is outside your employed work or in relation to professional matters where the employer may not be willing to represent you (e.g. Coroner Court).

Telehealth

COVID-19 accelerated the implementation and delivery of telehealth services across Australia. This increased usage has created new clinico-legal risks for healthcare practitioners.

How to mitigate your clinico-legal risk

- Only provide telehealth services when clinically safe and appropriate to do so. Diagnostic error is one of the major risks associated to telehealth consultations. Failure or delay in arriving to the correct diagnosis via telehealth can be avoided by being prepared to cease any telehealth consultation if you believe a face-to-face consultation is necessary, even if you are not the health practitioner who can provide it.
- Ensure you have adequate indemnity cover for the provision of telehealth services. MIPS provides cover for technology-based healthcare services on condition:
  - You and the patient are located in Australia.
  - Your practice is in accordance with AHPRA's, MBS and specialist colleges' requirements, guidelines and advice.
  - You hold current AHPRA healthcare practitioner registration.
  - You have appropriate training, experience and qualifications for the healthcare activities undertaken by you.
  - You have an appropriate membership classification for the healthcare activities undertaken by you.
- Follow your College and the MBA's guidelines to ensure you follow good practice principles when conducting telehealth consultations. For example:
  - Apply the usual principles for obtaining your patient's informed consent, protecting their privacy and rights to confidentially.
  - Evaluate the appropriateness of the telehealth-based patient consultation. Assess whether a direct physical examination is necessary.
  - Introduce yourself to all patients in a consultation. Identify all attendees in a consultation and document on your notes.
  - Follow up the progress of the patient and inform the patient's general practitioner or other relevant practitioners. Keep your colleagues well informed when sharing the care of patients.
  - Keep contemporaneous records of the consultation

- Always meet the requirements for Telehealth MBS items.

Medicare/PSR

MIPS has seen an increase in the number of notifications from members who have been contacted by Medicare seeking an audit of their billings. These audits arise from sophisticated electronic analysis which identify inaccurate or unusual billing profiles of healthcare providers across Australia. A large proportion of these are due to practitioners' lack of understanding and education about Medicare billing. In these instances, the issue can usually be resolved by engagement with further education and possibly the reimbursement of the amounts claimed.

In a smaller number of cases, unsual billing profiles are indefensible as there is no logical or practical explanation and/or patients' records to justify the items claimed. Those matters are often escalated by Medicare with potentially more punitive outcomes.

How to mitigate your clinico-legal risk

- Ensure you keep abreast of your obligations with Medicare and the MBSYou are fully accountable for ensuring that item numbers you use are applied lawfully. You must understand every item number and descriptor your practice employs and exercise your best judgement to interpret them.
- Medicare provides instructions including 10 strategies to assist practitioners . In summary:
  - Have designated staff whose role includes Medicare billing assurance responsibilities
  - Have documented Medicare billing procedures
  - Update and fully use your practice software
  - Have effective administrative record keeping in place
  - Notify the department in a timely manner when incorrect billing under Medicare has occurred
  - Encourage good communication between practitioners and other practice staff
  - Promote knowledge of Medicare billing assurance to all health professionals in your practice
  - Have senior management commit to Medicare billing assurance
  - Identify and remove workplace arrangements that may lead to incorrect billing under Medicare.
  - Check that your practice's requesting, and referral procedures are compliant with relevant legislative and regulatory frameworks.

Practice entity/Cyber risk

Practices and not just practitioners can be the victim of a civil action (ie being sued). You can insure your business/practice to cover the legal defence costs of any claim made against your practice and damages a court may order a practice to pay. Practice indemnity coverage, including a cyber risk cover, should be a part of any business risk management strategy to protect what you have worked so hard to build.

Cybersecurity in healthcare is of increasing concern . Healthcare organisations are attractive targets for cybercrime for two main reasons:

- they are a rich source of highly prized personal information
- its defences are comparatively weak.

Ensuring your practice is correctly equipped to provide IT and online security is essential to protect your staff, your practice, yourself and most importantly, your patients from loss or theft of data and/or sensitive information.

How to mitigate your clinico-legal risk

- Do not freely disclose personal, financial or credit card information. Always verify the authenticity of a caller or email sender before disclosing information.
- Enter or view sensitive information (passwords, patient details) prudently, make sure that no one else is watching.
- Always use strong passwords. Never repeat a password that you have previously used for Facebook, email or other online systems. Change your passwords regularly and never use the browser option to 'remember' your password.
- Be prudent in your approach to links received in emails and other communication. Be alert for websites that purport to be another website but do not have a correct website address.
- Become familiar with your internet browser and the features which verify a website's authenticity, for example many browsers include a green highlight or a closed padlock to indicate a secure connection. Refer to your browser online help.
- You should monitor your account transactions and other online systems on a regular basis to ensure that activity is consistent with your own.
- Never ask nor provide any information in relation to passwords, PIN numbers of other security details. A reputable organisation will never request this information.
- Ensure that all computers accessing your Cloud service are protected by a firewall and anti-virus program. Make sure you keep your security programs up to date and renew your subscriptions.

If you're concerned your clinic is exposed to the multitude of risks associated with ownership and operation, MIPS has established

a relationship with Aon to help MIPS members to consider and acquire practice entity and cyber cover. Aon have developed Healthcare Clinic Malpractice cover specifically for the Australian market. Further information can be found here.

Related articles

CAREER LEADERSHIP PROGRAM >