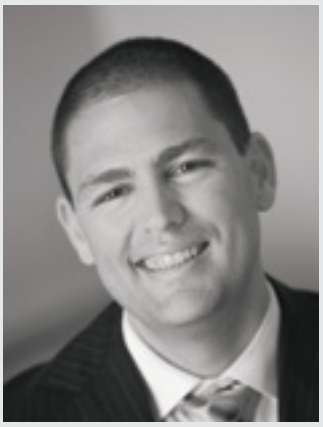
Managing the risks of practice growth



CHRIS MARIANI
Director, Medical & General Risk Solutions

M: 0419 017 011

E: chris@mgrs.com.au

Authorised Representative Number: 434578

MGR
MEDICAL AND GENERAL RISK SOLUTIONS

Many large multi-doctor medical practices start out life as small solo-doctor practices with perhaps a receptionist and nurse. The doctor-owner is able to control many of the elements of the practice and often directly oversees most, if not all, of the 'goings-on' in the practice.

As the practice quickly grows, the same level of oversight is simply not possible. As a result, the doctor delegates control to staff, becomes increasingly busy with patients and as the saying goes – spends time in the business, rather than on the business. This creates numerous risks and without the right risk management strategies and insurances, leaves the practice exposed.

The following example perfectly illustrates the risk of growth. This is from DUAL Insurance – who should have known better considering they provide an insurance product ('Management Liability') which covers a company against employee fraud:

> *In a much talked-about session, the Asia-Pacific CEO took to the stage to spell out how an employee siphoned off $17 million, offering a warning that it could happen to any business. "The trauma that DUAL has been through in the last three months is something I'd never want any business to go through." On 30 June, news broke that former employee Josie Gonzalez and her husband had allegedly misappropriated $17 million in insurer funds, via false invoices to a fictitious law firm, JAAG.*
>
> *Coates says the problem was DUAL's processes hadn't kept up with its growth. "When I first set up DUAL I was approving every invoice. I wanted to know where every dollar went. As the business had grown, our two bank signatories were signing 800 invoices a month," he says.*
>
> *"Many CEOs have asked me how we uncovered it, saying surely it was an issue of annual leave. It wasn't at all and any of us who are running businesses and thinking annual leave is a logical way in the current technological age we live in to prevent fraud, is living in a different world. That control doesn't work. No-one is ever really on holidays. We can still check out emails and keep the business going." Coates says Gonzalez took every day of her annual leave.*
>
> *"If you're serious about annual leave as a control you have to do what the banks do: for two weeks of their four weeks' annual leave they block every single person's system access," he says. The fraud was uncovered because Gonzalez's access to the system was blocked for part of her time on maternity leave.*

The employee fraud case above could equally occur in a medical practice – and frequently does. We speak at numerous doctor conferences annually and most times at least one doctor in the room will raise their hand to say they, or a colleague, were the victim of employee fraud. We are also seeing fraud by cyber criminals on the rise, and now is the time to tighten your financial controls and oversight.

There is no easy solution to safeguard a medical practice from risk. There are however, steps every practice can take and the following is our philosophy on managing risks in a medical practice.

Insurance is only part of the solution - structure first, then risk management, insurance is last!

Not everything is insurable. No amount of insurance can protect a doctor's largest risks – their medical registration and reputation. Insurance should be a part of your 'risk management framework'. Get advice from relevant experts on mitigating your key risks –accountants, lawyers, risk managers, insurance brokers, financial planners, IT consultants, medical billing experts, etc. Think in terms of "what can I do to protect my assets, liabilities, reputation and revenue?" Aim for three levels of protection:

1. First layer – asset protection/structure – what can you do to protect assets?
2. Second layer – risk management – identify and manage your risks.
3. Third layer –insurance – purchase the right insurances to cover your key insurable risks.

Spend your money on the right insurances

Don't insure the small stuff. There is also no point buying the cheapest policy if it doesn't provide the cover needed. You might as well stick your money in the bank and self-insure! Understand what insurances you're required to have by law or contract. Consider what other policies you may benefit from and judge these against your other risk management options – e.g. should I spend $1,000 on that insurance policy or spend it on my IT system to improve my backup, cybersecurity and IT supplier response times?

HERE ARE SOME STEPS FOR PRACTICE MANAGERS CAN TAKE TO HANDLE RISKS IN THEIR MEDICAL PRACTICE.

Start with your top 10 risks

Do you know the top 10 risks in your practice? How are you managing these risks? What would be the financial loss, reputational damage or other consequence? What experts could you call on to assist should the risk eventuate? Conduct a workshop with your staff and brainstorm risks. Speak to other practices and experienced people who can share their insights and experience. Develop a risk framework with management oversight. Your top 10 risks should be written into a *'Risk Register'* and reviewed and actioned at regular management meetings. Break your risks into key areas such as the following example:

Risk area: IT and key equipment

What could go wrong:

- Power outage
- Breakdown
- Cyber attack
- Privacy breach
- Virus
- Loss of key supplier
- Back-up failure

Existing controls: Document the existing controls in place such as having a documented Disaster Recovery and Business Interruption Plan, service agreements with suppliers, annual IT security reviews, etc.

Actions: Document what else you need to do, by whom and when.

Don't DIY insurance – this also applies to advice from other experts such as lawyers, accountants, financial planners, IT consultants, etc.

You have as much chance of getting it right as I do of performing neurosurgery on myself! You simply don't know what you don't know. You're far better off focussing on your core skills and outsourcing the rest. The pharmacists' "best stuff" is behind the counter and only accessed with a prescription. Insurance is often the same. Many of the best business insurers (and policies) are only available if you have a script –aka an insurance broker/adviser. You should also be seeking advice – so ask "what insurances do you recommend, are you providing me personal advice and is your duty to me or to the insurer?"

Prevention is better than cure (but it's hard to cure the unknown)

I once visited a paper-based psychiatry practice. They had been running for over 30 years and their medical records room was down an unsupervised corridor with patient toilets at the end. There was no door, let alone a lock to the medical records room. After some appropriate (risk management) counselling, they had a door and lock installed – far cheaper than the potential $1.7 million fine under Australian privacy laws. Even though they had walked past the risk every day, it never occurred to them they were not managing their risks appropriately; they were completely ignorant to the huge fine and huge risk staring at them every time they walked past.