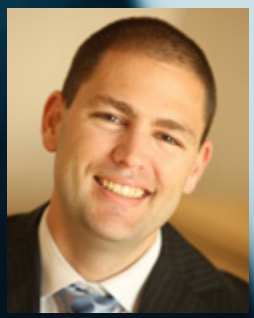
Are you complying with Australian privacy law?

Compliance with privacy laws has now become a risk management issue. **Chris Mariani** guides us through the new legislation and what we need to comply.



Chris Mariani is Director at Medical and General Risk Solutions.

In the 2014 Winter edition of the Private Practice magazine I discussed the changes to Australian privacy laws, which came into effect 12 March 2014. The changes brought increased obligations and risks to business and in particular to healthcare practices and practitioners.

Consider the below question and range of answers. How would your practice answer this question? If not something along the lines of Answer C, then you and your practice are potentially at increased risk of civil penalties, patient complaints and legal action, and reputational damage.

QUESTION:

"Dear doctor, can you please provide me a copy of your Privacy Policy, how do you make is accessible to patients and tell me about your processes to protect patient privacy?"

The answer usually falls into three categories:

ANSWERS

A. *"What's a Privacy Policy and should I have one?"*
(the most common answer)

B. *"We have one somewhere, but I have no idea where it is or when we last looked at it. The practice manager is responsible for privacy"*

C. *"We recently updated our Privacy Policy, we put it on our website and also a hard copy at reception. We have detailed processes for privacy and embed it into the business. It is a regular item on our management team meetings and it's included in our staff induction and training process. We are all responsible for patient privacy, but Mary takes the lead as the appointed Privacy Officer"*
(the least common answer, but obviously the best!)

The third answer is the right answer from a risk management perspective. Unfortunately as noted, this is really the answer I hear, but it is not too late to put in place systems and processes.

Medical practices hold sensitive patient information and as a result are often targeted by cyber criminals. Many as seen as 'low hanging fruit' given their relative spend on IT security compared to big business – and their reliance on patient data to continue business. Some reports suggest the chance of a cyber-attack are as high as 1 in 5. In addition to cyber risks, privacy breaches can also occur due to hard copy patient records being lost or stolen, or breaches at the reception desk due to poor processes or a lack of understanding of privacy obligations by front line staff.

See table over >

If you have any questions or need advice on your insurances, please contact Chris Mariani on (02) 9905 7005 or 0419 017 011, or email **chris@mgrs.com.au** for an obligation-free discussion and review.

QUESTION	ANSWER
What is a Privacy Policy?	Wikipedia defines a privacy policy as a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. In Australia, privacy law is found within the Privacy Act (1988) and now includes 13 Australian Privacy Principles (APPs) which can be found at http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles
Do I need a Privacy Policy?	Yes, if you are a "health service provider" (e.g. a medical practice or a medical practitioner set up as a sole trader), then you are required to have a Privacy Policy and comply with the Privacy Act. For most Australian businesses, they are only subject to the Privacy Act when their turnover reaches $3million. However this $3 million does not apply to healthcare businesses.
Where can I find more information about the Privacy Act and where can I get assistance or advice?	The Office of the Information Commissioner website contains lots of useful information and tools http://www.oaic.gov.au/ Also consider your MDO or the AMA who may be able to provide you with a template Privacy Policy or other support. For a risk audit of your practice, please feel free to contact Chris Mariani on 0419 017 011 or chris@mgrs.com.au
What are the risks and am I insured?	There are numerous risks for a medical practice which include: • A patient brings a civil compensation claim alleging a privacy breach. This risk should be covered by a doctors or practices medical indemnity insurance, but check your policy to make sure. • A complaint is made to the Privacy Commissioner. The legal fees may be covered by a doctors or practices medical indemnity insurance, or under other policies such as Management Liability and Cyber Risks. • The Privacy Commission seeks a civil penalty against the practice and directors. This is not currently covered by most medical indemnity policies and usually cover is required under a Management Liability or Cyber Risks policy. • A successful cyber-attack results in lost income and IT costs to recover your data. This risk is usually only covered in a Cyber Risks policy. There are many other potential risks such as reputational damage. Its important mitigate your risks and hold the right insurances.
We run a cloud based IT solution with patient data stored in the cloud. Is that an issue?	Not if managed correctly where you take steps to mitigate your risks. Note you are still responsible for patient privacy, so you need to ensure your IT suppliers take reasonable steps to protect patient privacy. There should be a contract in place where they agree to indemnify you for their negligent acts. If any patient data will be stored or sent overseas, you also need to be aware of APP 8 — Cross-border disclosure of personal information. This needs to be reflected in your Privacy Policy. Ask your IT consultant where your patient data is stored. Consider an independent consultant audit.
We collect patient data to be used in a research study. Is this ok?	You should inform the patient you plan to use their de-identified data in a research study or for another secondary purpose. This would be best done verbally and as part of your patient information form and your Privacy Policy.
We have developed our Privacy Policy. Where should we put it?	The best place is as a combination of having it on your website and hard copy supplies kept at reception. Also consider putting a statement on your patient information form *"we take your privacy seriously, a copy of our Privacy Policy is available from reception or our website…"*