UP TO SPEED?

Chris Mariani is Director at Medical and General Risk Solutions.

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.

If you are running a healthcare business then you should have recently updated your privacy policy and put in place systems and processes to ensure you comply with the privacy law changes that came into effect 12 March 2014.

It's important to note all businesses that provide a 'health service' are captured by the privacy laws (other private businesses are only captured when their turnover is greater than $3 million annually).

If you are not up to speed on the privacy laws a good place to start is the website of The Office of the Australian Information Commissioner (OIC) **www.oaic.gov.au/privacy** (formerly the Privacy Commissioner) and in particular the 13 Australian Privacy Principles (APPs):

- **APP 1 – Open and transparent management of personal information**
  Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
- **APP 2 – Anonymity and pseudonymity**
  Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
- **APP 3 – Collection of solicited personal information**
  Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.
- **APP 4 – Dealing with unsolicited personal information**
  Outlines how APP entities must deal with unsolicited personal information.
- **APP 5 – Notification of the collection of personal information**
  Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.
- **APP 6 – Use or disclosure of personal information**
  Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
- **APP 7 – Direct marketing**
  An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
- **APP 8 – Cross-border disclosure of personal information**
  Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
- **APP 9 – Adoption, use or disclosure of government related identifiers**
  Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
- **APP 10 – Quality of personal information**
  An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
- **APP 11 – Security of personal information**
  An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
- **APP 12 – Access to personal information**
  Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
- **APP 13 – Correction of personal information**
  Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

The privacy changes also provide additional powers to the OIC, such as to conduct assessments of privacy performance for businesses. One of the new risks is the OIC's ability to seek a 'civil penalty' for serious or repeated offenses of up to $340,000 for individuals and $1.7 million for entities. It's important to note that 'civil penalties' are generally not covered by medical indemnity policies – unless there is specific cover usually referred to as 'Statutory Fines and Penalties'. This cover is however

available outside of medical indemnity policies, so please contact us if you require advice or have any queries.

NO DOOR, NO DEFENCE...

Recently I visited a specialist medical practice. They had been in business for many years and were still on paper medical records. The medical records room was off the main corridor leading to the toilets, and the room had no door. Patients and visitors had easy access to the records room as they moved freely down the corridor.

Imagine a person decided to take a few records and then post these on the web and the impacted patients bring a privacy claim against the doctors/practice. This type of claim would likely be covered by the doctors/practice policy (as it is a compensation claim). But from 12 March 2014, the OIC now has the powers to seek a civil penalty against the doctors and/or practice. A civil penalty is a penalty applied to deter bad behaviour, so the practice would be well served to take reasonable steps such as installing a lockable door and considering other reasonable steps to protect the medical records. The same applies to computer based records. Having up to date virus protection, firewalls, third party agreements and other security measures are all part of good risk management.

APP 11 states an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure...

What practical things can you do to ensure you comply with the privacy laws?

1. There is a wealth of information at Office of the Australian information commissioner website at: **www.oaic.gov.au/privacy**
2. Speak with your Medical Defence Organisation or your state AMA. Some are running sessions on this topic and have may be able to provide you with templates and other tools.
3. Speak with your IT consultants and have them review and provide advice on how to prevent or minimise the risks of data breaches.
4. Review your physical security particularly where you have paper based patient records.
5. Should you use third parties to store or destroy patient records ensure there is a written contract that requires the third party to comply with the privacy laws. Consider indemnities and seek legal advice.
6. Appoint a person in your practice to be responsible for privacy.
7. Speak to your insurance broker or adviser and ask for advice on how to protect yourself with the right insurances. Ⓟ

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.