

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs

Via online submission

Dear colleagues

**General Enquiries
and Client Service**

P 1800 777 156

F 1800 839 284

**Claims and Legal
Services**

P 1800 839 280

F 1800 839 281

www.miga.com.au

miga@miga.com.au

Postal Address

GPO Box 2048, Adelaide
South Australia 5001

MIGA submission – Cyber security regulation in healthcare and insurance

As a medical defence organisation and professional indemnity insurer, MIGA appreciates the opportunities to contribute to the Department's discussion paper, *Strengthening Australia's cyber security regulations and incentives*, and to meet with Department officials about the issues it raises for both healthcare and insurance.

MIGA's position

Cyber security expectations for the healthcare and insurance sectors must be realistic, proportionate and practical. They should be sector-specific, co-designed with stakeholders. A 'one-size-fits-all', economy-wide approach to cybersecurity is inappropriate.

For both healthcare and insurance, the Commonwealth *Privacy Act* provides a sufficient, fit for purpose framework of high level expectations, which can (or already have been) developed further through sector-specific guidance.

In the healthcare sector there are

- Variable capacities of a broad range of healthcare providers to deal with cyber security risks
- Significant risks of providers disengaging from digital health initiatives if regulatory expectations and burdens are unrealistic and impractical for both themselves and their patients.

MIGA sees a greater role for government, regulators and technology providers to assist healthcare providers with ensuring appropriate cyber security, including through product certification, ongoing obligations on technology providers and providing more specific information / guidance for the healthcare sector.

MIGA does not support additional remedies for breaches of cyber security standards. What is already in place for both healthcare and insurance is sufficient.

MIGA's interest

MIGA advises, assists, educates and advocates for doctors, medical students, healthcare organisations and privately practising midwives throughout Australia.

With over 36,000 members across the country, it has represented the medical profession for over 121 years and the broader healthcare profession for more than 18 years.

It regularly advises its members and clients on cyber security and privacy issues, and educates doctors and other healthcare providers on medico-legal and risk management issues around cyber security and privacy.

MIGA has been involved in a wide range of regulatory and policy work dealing with cybersecurity, including the Commonwealth Attorney-General's review of the *Privacy Act* and consultation on serious data breach notification, the ACCC's Digital Platforms Inquiry, OAIC's consultations on its health privacy guidance and notifiable data breach scheme resources, and ongoing engagement with the Australian Digital Health Agency.

Fit for purpose regulation for healthcare

It is important that cyber security regulation on healthcare providers does not become unnecessarily proscriptive.

The ability to meet significant new privacy obligations would vary significantly across the healthcare sector. This raises the potential for adverse flow-on effects to patients, including issues around access to, and affordability of, healthcare.

The indication on p15 of the discussion paper that “*The Privacy Act does not apply to businesses with a revenue less than \$3 million*” is incorrect in the context of healthcare.

The *Privacy Act* applies to all private sector health service providers, irrespective of size or turnover. It applies to the solo GP in the same way it does to the large private hospital.

As indicated in its [submission](#) to the Attorney-General’s review of the *Privacy Act*, MIGA considers a separate privacy regime is required for healthcare.

Healthcare already has additional, distinct regulatory privacy regimes which involve cybersecurity expectations, including

- Professional disciplinary board codes and guidelines – for doctors these include
 - o *Good Medical Practice – A Code of Conduct for Doctors in Australia*
 - o *Guidelines for technology-based patient consultations*
 - o *Social media policy*¹

These are enforceable under the *Health Practitioner Regulation National Law*.² Professional regulatory tribunals have powers to order pecuniary penalties, suspension or cancellation of registration and place a broad range of restrictions and other conditions on a provider’s practice³

- Various professional ethics codes, such as the Australian Medical Association *Code of Ethics*
- Professional college and association codes of conduct enforceable through disciplinary processes
- Employer / healthcare entity codes of conduct / procedures enforceable through disciplinary processes
- Common law duties of care to patients, which include confidentiality obligations
- Obligations under contract and equity relating to patient confidentiality.

MIGA does not see these regimes as reflective of the comment on p12 of the discussion paper that “*In most cases, the application of these laws to cyber security is theoretical and unlikely to occur in practice*”. It submits that this comment is misleading and incorrect.

Healthcare regulation already places great emphasis on privacy, with significant consequences for breaches of its expectations.

Within that context, cyber security expectations should be tailored for healthcare, utilising guidance and examples of good practice from regulators, co-designed with stakeholders.

The OAIC’s *Guide to health privacy* provides an example of a potential approach in the context of broader healthcare privacy issues which could be adopted for healthcare cyber security.

A range of helpful cyber security guidance is already provided by the Australian Digital Health Agency through its Cyber Security Centre.

The concept of cyber security health checks for small business, co-designed with the healthcare sector, is worthy of further analysis and consideration. Any check for the healthcare sector should be developed through existing channels and utilise key resources from healthcare peak bodies, such as the RACGP’s *Information security in general practice*.

¹ These codes and guidelines are available at www.medicalboard.gov.au/Codes-Guidelines-Policies.aspx - similar codes and guidelines are in place for other registered health practitioners

² Section 41, *Health Practitioner Regulation National Law*

³ Section 196, *Health Practitioner Regulation National Law*

Fit for purpose regulation for insurance

As the discussion paper recognises, insurers and other prudentially regulated entities are subject to the Australian Prudential Regulatory Authority (APRA) Prudential Standard CPS 234, *Information Security*, made under s 32 of the *Insurance Act 1973* (Cth).

CPS 234 is a good example of an appropriate sector-specific approach. It

- Sets out clear expectations and responsibilities
- Provides a flexible compliance model based on scales of risk and capability
- Can be supplemented by additional guidance and examples of good practice as needed over time in response to emerging or recurring issues.

Whilst this approach is not necessarily suitable for all sectors (particularly as it governs a group of entities with significant financial capabilities), it reinforces the importance and value of sector-specific approaches, co-designed and / or developed in consultation with the relevant sector.

In addition s 912A of the *Corporations Act 2001* (Cth) offers a further regime of cybersecurity regulation applying to insurers as Australian Financial Services Licensees.

Given each of CPS 234, *Corporations Act* mechanisms and the *Privacy Act*, it would be thoroughly inappropriate to enact another layer of cyber security regulation on insurers.

Realistic expectations for healthcare

Cybersecurity regulation for healthcare needs to be

- Realistic for the wide range of healthcare providers
- Commensurate to the degree of risk they face.

Healthcare providers range from solo GPs in remote areas through to large, full-service hospitals in capital cities, with a broad range of entities and capabilities in between.

For many smaller healthcare providers, it is not an issue of deciding against investing in cyber security or weak commercial incentives, but rather limitations of time and resources in what they can realistically do.

MIGA is concerned that a 'minimum controls' approach could be used to prescribe certain cybersecurity expectations which are inappropriate and unworkable for the broad range of healthcare providers.

'Secure by design' principles are generally more a matter for technology providers, rather than healthcare providers using that technology.

Accordingly MIGA opposes a cyber security code setting out minimum standards for reasonable steps to protect personal information in healthcare under APP 11 of the *Privacy Act*.

The implications of the COVID-19 pandemic for healthcare illustrate the challenges around ensuring a fit-for-purpose cyber security regime for healthcare. Existing regimes created uncertainty around appropriate use of telehealth platforms, and the roll-out of digital image and electronic prescribing. This was unhelpful for providers and patients and impeded uptake of important channels to provide healthcare in difficult times. This must be avoided in future privacy and cyber security regulation.

Discouraging digital initiatives in healthcare

MIGA is concerned that non-healthcare related issues are driving certain views on expectations for healthcare cyber security.

This creates misapprehensions and undue concerns about use of digital health initiatives, such as telehealth, and other commonly used communication methods, including email and SMS.

Many patients prefer to use relatively simple, straightforward communication methods, such as email and SMS, for communications about their healthcare, and to use widely used platforms, such as Zoom and Facetime, for telehealth.

Prioritising adoption of controls such as encryption of data and multi-factor authentication can be more challenging for both smaller healthcare providers and patients themselves.

Until there are reliable secure messaging and bespoke healthcare telehealth platform methods readily available and easily used by healthcare providers and patients alike, cyber security expectations in healthcare must allow for more commonly used technologies.

The best way to ensure strong passwords and timely application of critical patches is to ensure healthcare providers are given simple, easy ways of taking these steps.

Role of government, regulators and technology providers in healthcare

MIGA sees a greater role for government, regulators and technology providers in supporting cyber security in the healthcare sector.

There is scope for government to indicate whether various overseas cyber security regulatory regimes comply with the *Privacy Act*. There are already significant uncertainties around the use of digital health technologies which may involve an overseas element, such as cloud storage systems and telehealth platforms. Expectations on healthcare providers around issues of accountability, control and security in these situations are unduly burdensome. They cannot be expected to be legal or IT experts, ensuring that overseas entities comply with the *Privacy Act*.

Compliance activities by regulators, particularly in healthcare, should emphasise an 'education-first approach', explaining expectations and assisting with compliance. This approach is already used successfully by other regulators in the healthcare context, including by the Australian Health Practitioner Regulation Agency (Ahpra) and the National Boards for professional discipline, the Therapeutic Goods Agency (TGA) for advertising, and various state / territory health departments for prescription medications regulation.

For technology providers MIGA endorses the following observations on pp10 and 11 of the discussion paper

Unfortunately, end users almost always have less capability to manage cyber security risk compared to the technology companies that supplied the software or device.

... most buyers don't have the technical capability to determine the security of a product. Even with technical capability, it is costly and time-consuming for buyers to independently verify the security of products.

Appropriately managing cyber security requires significant input from technology providers, particularly use of 'secure by design' principles.

MIGA sees a need for technology providers to take responsibility for addressing issues which are often beyond the capabilities of individuals and business, including indication where technologies comply with certain cybersecurity expectations.

Remedies for cyber security breaches in healthcare and insurance

Current enforcement frameworks and remedies for any healthcare privacy breaches are sufficient.

There is no basis for additional enforcement, direct action rights or a statutory privacy tort for healthcare.

No evidence has been offered of shortcomings in the healthcare sector, particularly the ability of patients and other affected individuals to seek remedies for privacy breaches.

Duties at common law and equity that healthcare providers owe their patients provide a framework for bringing direct actions in healthcare, whether in tort or otherwise. This rarely exists in most other sectors. Breaches of duty can lead to damages awards.

In addition the OAIC has the ability to award compensation for both financial and non-financial loss.

The relative paucity of such claims, both publicly reported and in MIGA's experience, suggests either

- Remedies available under existing *Privacy Act* and other state and territory regimes are sufficient
- There is already a more robust and workable system in place for appropriately handling healthcare information.

MIGA strongly supports a *Privacy Act* enforcement model based on escalation. Civil penalties are rarely, if ever, appropriate in a healthcare context. Changing the enforcement model in healthcare poses significant risks of digital health disengagement by healthcare providers.

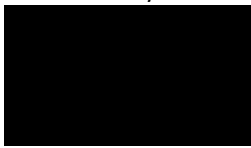
For a wide range of general insurances, including medical indemnity insurance which is the focus of MIGA's business, its insured members and clients can seek redress directly through the Australian Financial Complaints Authority (AFCA) for breaches of the *Privacy Act*. Available remedies include compensation for both financial and non-financial loss. There is nothing to suggest anything more is required in this context.

Next steps

If you have any questions or would like to discuss, please contact Timothy Bowen, [REDACTED] / [REDACTED].

We look forward to remaining engaged with the Department on the progress of this work.

Yours sincerely



Timothy Bowen
Manager - Advocacy & Legal Services



Mandy Anderson
CEO & Managing Director