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

23 March 2020

Mrs Lucy Wicks MP
Chair, Joint Committee of Public Accounts and Audit
Parliament of Australia

Via email - jcpaa@aph.gov.au

Dear Mrs Wicks

MIGA submission – My Health Record cyber resilience

As a medical defence organisation and medical / professional indemnity insurer, MIGA appreciates the opportunity to contribute to Committee's inquiry into the Auditor-General's Report No 13 (2019-20), *Implementation of the My Health Record System*, focusing on cyber resilience issues.

MIGA's submission focuses on recommendations 2 and 4 of the Auditor-General's report, relating to monitoring health provider compliance with My Health Record legislative requirements and use of the system in emergency situations.

Executive summary

MIGA supports the ongoing development and use of the My Health Record system, which has potential to contribute to improvements in Australian healthcare.

It supports

- Ensuring all eHealth platforms, including My Health Record, can continue to improve and develop to reflect the evolving needs and realities of Australian healthcare
- Ensuring regulatory frameworks and other obligations relating to both My Health Record and eHealth more generally, particularly around privacy and confidentiality, remain fair, practical and fit for purpose, and harmonised with other medico-legal requirements on Australian healthcare providers.

MIGA believes there are a range of broader issues that put the Auditor-General's findings and recommendations on My Health Record cybersecurity risks and emergency access into context. This is a key part of considering responses to the Auditor-General's report.

MIGA's interest

With over 34,000 members, MIGA has represented the medical profession for almost 120 years and the broader healthcare profession for 17 years.

MIGA has significant interest and expertise in eHealth issues, which intersects with the My Health Record system and digital health / eHealth more broadly in a range of ways.

It regularly advises and assists its members and clients on these issues in various medico-legal and other health regulatory contexts. It delivers education to its members and the broader health profession on these issues.

MIGA's advocacy and engagement work spans eHealth issues across the country. It has been engaging with Australian Digital Health Agency (**AHDA**) around My Health Record over several years. It contributed to the Senate's inquiry into My Health Record. Its broader advocacy and engagement work covers issues such as digital health strategy, inter-operability, digital platforms, privacy, notifiable data breach, public hospital eHealth systems and artificial intelligence. It has contributed to the work of the Treasury and Attorney-General, the Office of the Australian Information Commissioner, Australian Human Rights Commission, state health departments and professional bodies.

My Health Record – a wide range of regulatory frameworks

Any consideration of My Health Record cyber resilience and both privacy and security more broadly needs to include the wide range of existing regulatory, professional and ethical frameworks for doctors and other healthcare providers in using My Health Record.

These frameworks go beyond the My Health Record legislative regime, the privacy / security controls within My Health Record itself and the "*external environment controls*" mentioned by the ADHA in its response to the Auditor-General's report.

These additional frameworks include

- The *Health Practitioner Regulation National Law* (**the National Law**)
- Professional codes and standards
    - For doctors these include the Medical Board's *Good Medical Practice – A Code of Conduct for Doctors in Australia* and the Australian Medical Association *Code of Ethics* – comparable codes and standards exist for other health professions
    - Breaches of these codes and standards can lead to disciplinary action under the National Law, or be used in support of a civil damages claim
- The Commonwealth *Privacy Act*, which provides a regulatory and enforcement framework including remedies such as enforceable determinations or undertakings, injunctions and financial penalties
- Civil law standards of care and confidentiality obligations, breaches of which can lead to damages awards.

Shared cybersecurity risks

It is imperative that expectations of healthcare providers around cybersecurity for My Health Record, and eHealth more generally, are sensible, fair and practical.

MIGA is conscious of the rationale for monitoring compliance by healthcare providers with My Health Record legislated security requirements. It is concerned about potential for this to

- Not recognise the existing broad privacy and security obligations (as set out above)
- Become something that appears distrustful of and punitive towards doctors and other healthcare providers.

A Medicare-style monitoring and compliance system is unnecessary. It would likely discourage healthcare providers from engaging with My Health Record.

MIGA is encouraged by the ADHA's recognition of the existing "*environment of controls*" including privacy laws, professional standards and risk systems, and its commitment to considering this "*complex environment*" when working with stakeholders to raise standards in health information management. It looks forward to working with the ADHA on these issues.

The ADHA's intent to "*lift the capability of the health sector to continue to meet increasing community expectations on privacy and the security of health information*" must reflect the reality of how seriously and sensitively doctors and other healthcare providers already treat health information. The laws, ethics and professional standards of the healthcare professions reflect high levels of privacy and security around health information. It is vital to both appreciate and account for this sufficiently.

Although the private healthcare sector reported the most notifiable data breaches of any sector in 2018, this does not of itself mean there are significant concerns around healthcare cybersecurity. It is imperative to appreciate the context of broader notification obligations in healthcare, and the sheer number of healthcare services provided each and every day.

Private healthcare is one of the very few sectors where notifiable data breach and broader *Privacy Act* obligations apply to all healthcare providers, irrespective of size. For most other sectors these obligations only apply to organisations with a turnover of greater than $3 million per annum.

Before the notifiable data breach regime commenced, there was a concerted education campaign by the ADHA and professional healthcare stakeholders (including MIGA) to explain to healthcare providers what their obligations were. This did not occur in all affected sectors.

These factors meant far greater scope for notifiable data breaches to occur, and far greater understanding of notification obligations, than in most other sectors.

Comparatively higher levels of notifiable data breaches are understandable. They are not suggestive of a broader cybersecurity problem in healthcare.

It is imperative that My Health Record security and compliance controls be sensible, practical and fair.

Legislated security requirements for My Health Record can be interpreted in a broad range of ways. Unfortunately they can be used to argue for unreasonable expectations on healthcare providers which are unwarranted and which were never intended.

Any compliance monitoring strategies should be developed in consultation with key professional stakeholders, including medical defence organisations.

Emergency access to My Health Record

MIGA recognises the need to ensure that emergency access to My Health Record only occurs in situations where it is both permissible and warranted.

MIGA is troubled by any presumption that use of the emergency access function could constitute an interference with privacy.

Emergency access to My Health Record is contemplated where

- There is a serious threat to the individual's life, health or safety and their consent cannot be obtained, or
- There are reasonable grounds to believe that access to the My Health Record of that person is necessary to lessen or prevent a serious threat to public health or safety.

Across Australia, serious threats to a patient's life, health or safety occur throughout any given day, particularly in hospital settings.

It is important to remember the context of when such access is contemplated – emergency situations – where critical decisions are being made in a very short space of time.

MIGA suspects that most, if not all, circumstances of emergency access to My Health Record by doctors and other healthcare providers were necessary. The numbers referred to by the Auditor-General appear consistent with what MIGA would expect as a level of appropriate emergency access to My Health Record.

The following also puts the numbers of My Health Record emergency access (80 in July 2018 and 205 in March 2019) in context

- Almost 36 million Medicare services per month in 2018-19[1]
- Over 900,000 hospital admissions per month in 2017-18[2]
- Over 666,000 public hospital emergency department presentations per month, an average of around 22,000 per day[3]
- The initial number of 80 emergency accesses in a month was before the My Health Record opt out period and the increased number of 205 was after the opt out period and significant professional and community education campaign on the use of My Health Record. With increasing use and awareness of My Health Record it would be reasonable to expect situations of emergency access to increase.

In addition it would be reasonable to expect that those with significant health problems, more likely to cause emergency situations, are more likely to actively use My Health Record given their interest in ensuring all necessary information is available to their healthcare providers when needed.

With the range of privacy frameworks in place (as set out above) and the My Health Record legislative regime involving significant civil and pecuniary penalties for unauthorised access to a My Health Record, it is difficult to see how healthcare providers would contemplate using an emergency access function without a proper justification.

[1] Services Australia 2018-19 Annual Report, p 3
[2] Australian Institute of Health and Welfare, *Admitted patient care 2017-18*, p 8
[3] Australian Institute of Health and Welfare, *Emergency department care 2017-18*, p v

The Auditor-General's report appears to contain a presumption that emergency access is only justified in situations where there is an access control set for a patient's whole My Health Record, not just for specific documents. MIGA disagrees with any such presumption.

Whilst it seems the emergency access function has been used much more for individual documents than the entirety of a patient's My Health Record itself, it does not follow that access to those individual documents was unwarranted.

In a time critical situation like an emergency where it is unclear what may be available in a restricted document, doctors and other healthcare providers may need to see a document first before they can determine whether it contains something that may assist in the emergency.

If you have any questions or would like to discuss, please contact Timothy Bowen,

Yours faithfully

Timothy Bowen
Senior Solicitor – Advocacy, Claims & Education

Cheryl McDonald
National Manager – Claims & Legal Services