Our Ref: MA:TJB

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

4 March 2016

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By email: privacy.consultation@ag.gov.au and post

Dear Colleagues

Re: MIGA submission to Serious Data Breach Notification Consultation

MIGA welcomes the opportunity to provide a submission to the Australian Government's consultation on the exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) (**the draft bill**).

Executive Summary

As a body which has regular involvement in health privacy issues, MIGA:

(a) has some concerns about what can be achieved by the draft bill and its proposed mandatory serious data breach scheme, but given the consideration already given to these issues focuses its submissions on practical issues relating to the scheme's operation;

(b) supports the 12 month period contemplated before the scheme begins operation, and proposes that it be used to develop clear guidelines dealing with the health care context, and to educate the health care sector on what it means for them;

(c) considers that issues relating to the broad range of health care contexts and thresholds for notification should be addressed in guidelines for the health care sector;

(d) opposes mandatory notification for any data breach involving health records , with notification in this context being based on notification threshold for the scheme generally; and

(e) would welcome the opportunity of working with the OAIC and other appropriate organisations on developing guidelines relating to operation of the scheme in the health context, educating health professionals and being part of ongoing review of the scheme operation.

Introduction

MIGA is a specialist insurer offering a range of medical indemnity insurance products and associated services to the health care profession across Australia. We insure medical practitioners, health care companies, privately practising midwives and medical students.

On a daily basis, MIGA's lawyers advise its members and policy holders on privacy issues, particularly confidentiality and disclosure of clinical records. We also have experience in advising our members and policy holders on the voluntary data breach notification scheme administered by the Office of the Australian Information Commissioner (**OAIC**) and in assisting our members and policy holders in making submissions to the OAIC on these issues. We also provided detailed submissions on the OAIC's review of health privacy guidelines last year.

MIGA makes this submission in its role as representing the interests of its members and policy holders.

Draft bill generally

At the outset, MIGA and its members and policy holders recognise the prime importance of security of health information such as clinical records, enshrined in the long-held principle of doctor-patient confidentiality. It supports a regime which protects individual privacy which does not impose an undue regulatory burden on the provision of health care, particularly for those medical practitioners who practise with limited administrative support.

MIGA has some reservations about a mandatory serious data breach notification scheme (**the scheme**), particularly what it can meaningfully achieve and how it will operate. We are concerned about the burden it may place on those who have to determine whether to make a notification and deal with its consequences.

However, MIGA notes the careful consideration given by the Australian Law Reform Commission to a mandatory serious data breach notification scheme, the wide stakeholder and public consultation undertaken on this issue, the increasing adoption of such schemes throughout the world and the proposal of a draft bill.

In those circumstances, MIGA focuses its submissions on the issues of practical operation of the scheme, and arrangements for ongoing review and oversight of the scheme.

Practical issues relating to the scheme

(a) Commencement date

MIGA supports the proposal in the draft bill, based on the ALRC's recommendation, for the operation of the scheme to commence 12 months after assent of the bill.

Our members and policy holders, other stakeholders and the public at large need time to understand, and prepare for, the operation of the scheme.

We are keen to ensure that this period is also used to develop clear guidelines, as contemplated by the discussion paper, addressing various issues arising in the health care context (particularly those we identify below) and to provide education to those in the health care sector on what it means for them.

We would invite the OAIC to consider engaging with both ourselves and other stakeholders during this period to discuss how to best educate the health care sector on these reforms.

(b) Acknowledging realities of data management

MIGA considers that careful consideration needs to be given by those exercising functions under the scheme in the health care context to the current realities of data management in that field.

MIGA's members and policy holders range from sole practitioners in rural areas, who have very limited administrative support and utilise paper-based record systems, through to larger group practices and clinics with considerable administrative and practice management resources, and sophisticated clinical record management (**CRM**) systems.

Amongst those members and policy holders who have adopted electronic CRM systems, there are a range of systems used, ranging from more basic password protected systems on a small number of computers, through to specialised systems on more developed networks, sometimes utilising cloud-based computing.

The provisions of the *Privacy Act 1988* (Cth) and the OAIC health guidelines contemplate a wide range of health data management systems which comply with legislative requirements, including both paper-based systems and sophisticated electronic systems with remote data storage.

Accordingly, given the pace of development of data management systems, some of our members and policy holders are more vulnerable than others to a serious data breach, such as through malicious hacking or inadvertent loss of data, despite their data security requirements complying with requirements of the *Privacy Act*.

In an ideal world, all health professionals and those working with them in the health care context would utilise the latest CRM systems. However, time, cost and other resource issues mean that having the most up to date CRM system is not a realistic expectation. These systems, and the scope for them to be hacked into, develop so rapidly that it is impossible to expect health care providers to be able to keep up to date with all these developments.

MIGA emphasises the need for careful and fulsome consideration to be given in determining appropriate management of a serious data breach, particularly in terms of considering whether to pursue penalty proceedings and in considering remedial action.

It may be that the development of internal OAIC notification handling guidelines, with input from appropriate stakeholders, would go a considerable way to addressing these considerations. MIGA would welcome the opportunity for both initial and ongoing input to such material.

(c) Determining 'serious data breach'

Implicitly, the term 'serious data breach' implies something significantly beyond a data breach of itself. It seems to be directed at the degree of unauthorised access to, or inadvertent loss or disclosure of, data.

In the health care context, this would seem to relate to a breach involving a large number of patients, or access to significant amounts of data about one or more patients.

Even in those situations, what constitutes a 'serious data breach' is not entirely clear.

Consider a scenario where a health care provider cannot locate one storage component containing backup data on a significant number of patients. If the CRM system uses up to date encryption technology it is highly unlikely the data would be accessible to unauthorised third parties. However, applying the test of 'likelihood of unauthorised access' does not necessarily assist in determining whether the 'lost' data constitutes a 'serious data breach'.

Alternatively, would the mistaken posting of a specialist's letter, containing a variety of information about a patient's health status, to the wrong hospital to that where a patient was treated, constitute a 'serious data breach'? The OAIC's Data breach notification guide cites the example of a pathologist sending a test result to the wrong GP as being an example of notification not occurring. However, this is in the context of information being sent direct to a person who has particular ethical duties, and not necessarily containing broader clinical information of particular sensitivity, such as mental health history.

Such examples represent a mere snapshot of the variety of different situations that health professionals may find themselves in when determining whether a serious data breach has occurred. Clearly, different minds will potentially judge such situations very differently absent further clarification.

Although it might be said that the second limb of the notification test, the 'risk of serious harm', is an important part of determining notification in these situations, a clear view needs to be able to be formed on each of the 'serious data breach' and 'serious risk of harm' thresholds independently.

In those circumstances, MIGA would support the OAIC exercising its function under Section 28(1)(a) of the *Privacy Act* to produce detailed guidelines, which include a variety of examples, which set out what it considers to be a 'serious data breach' in the health care context. MIGA would welcome the opportunity to contribute to the development and ongoing review of such guidelines.

Although the current OAIC Data breach notification guide is a useful starting point for developing appropriate guidelines, it is necessarily general in application, lacking specific guidance for the health care context. It would be worthwhile giving consideration to the development of other practical tools, such as 'yes / no' online questionnaires and also reference to examples, to assist people in understanding their obligations under the scheme.

(d) Determining 'risk of serious harm'

MIGA observes that the test for notification of a serious data breach, namely the risk of serious harm, is an inherently subjective test, over which reasonable minds will differ.

Obviously, there will be situations where it is clear that a mandatory data breach notification is required, such as intentional unauthorised access to clinical records with malicious intent.

Conversely, there will also be situations where it is clear such notification is not required, such as inadvertent access by IT professionals working on a CRM system at the request of a health care professional or organisation.

There will be a variety of situations where it is difficult for a health professional or organisation, and perhaps even those advising them, to determine if there is likely to be a risk of serious harm flowing from the serious data breach.

We understand that, if the bill is passed, the OAIC intends to issue guidelines on what constitutes a 'risk of serious harm'. Again, MIGA would welcome the opportunity to contribute to this process, as it has done previously with the OAIC in the context of reviewing the health privacy guidelines.

(e) Possible mandatory notification for any release of health records

Reference is made in the explanatory memorandum to the possibility of regulations specifying that any release of health information would be considered a serious data breach mandating notification.

MIGA acknowledges that health information is inherently sensitive information.

It is MIGA's position that such a step would be unnecessary and inappropriate, given the wide range of unintended disclosures of health information, both in terms of their degree of seriousness and risk imposed.

Such a requirement would impose an undue and overwhelming regulatory burden on health care professionals and organisations to require any unintended release of health information to be notified to the OAIC.

No basis has been offered, beyond the inherent sensitivity of health care information, warranting such a serious obligation. How such information is necessarily significantly more sensitive than other types of sensitive, personal information dealt with under the *Privacy Act* is not clearly apparent.

Further, we consider that such notifications could well exceed the doubling in notifications which OAIC contemplates under the new regime, meaning it may not be able to discharge properly its functions, and rightly focus on the cases involving serious data breaches posing a risk of serious harm.

Before any such obligation is considered, MIGA believes a careful examination of the risks and benefits of such an obligation, involving both quantitative and qualitative study, and detailed stakeholder engagement with the benefits of such study, is required.

Review and oversight of the scheme

For a new scheme such as the mandatory serious data breach notification scheme, it is important that its operation is subject to meaningful oversight and ongoing review by a variety of interests and from a variety of perspectives.

MIGA proposes the following:

(a) formation of an OAIC health stakeholder group:
    a. meeting perhaps on a six monthly basis;
    b. which considers issues relating to the operation of the scheme and potential improvement, including development of various guidelines; and
    c. including representatives from federal, state and territory health departments, representatives of peak health care organisations (such as the Australian Medical Associations and various professional colleges) and medical defence organisations such as MIGA;

(b) implementation of a regime of formal review, perhaps an initial three yearly, on the scheme operation in the health context, with appropriate scope for input from, and submission by, stakeholders and the public at large.

If you have any questions or require further consultation, please contact Timothy Bowen – Senior Solicitor – Advocacy, Claims & Education at timothy.bowen@miga.com.au, tel: 1800 839 280.

Yours sincerely

Mandy Anderson
CEO & Managing Director

Timothy Bowen
Senior Solicitor – Advocacy, Claims & Education