Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Avant Mutual Group Contact: Georgie Haysom Head of Advocacy
Contact details *(one or all of the following: postal address, email address or phone number)*	[contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? ~~YES /~~ NO

Your submission

About Avant

Avant Mutual Group Limited ("Avant") is Australia's leading medical defence organisation. It is a mutual organisation, owed by its members, and offers a range of insurance products and expert legal advice and assistance to over 68,000 medical and allied health practitioners and students in Australia. Our insurance products include medical indemnity insurance for individuals and practices, as well as private health insurance, which is offered through our subsidiary The Doctors' Health Fund Pty Limited.

Our members have access to medico-legal assistance via our Medico Legal Advisory Service. We have offices throughout Australia, and provide extensive risk advisory and education services to our members with the aim of reducing medico-legal risk and promoting good medical practice and patient safety.

We frequently advise our members on privacy issues, including steps to be taken if a privacy breach occurs.

Submission to 2012 consultation

Avant made a submission to the Attorney-General's 2012 Discussion Paper Australian Privacy Breach Notification. In that submission, we stated that our position on mandatory data breach notification was as follows:

1. *A mandatory data breach notification law should not be introduced.*
2. *The current position of voluntary data breach notification in accordance with the OAIC's April 2012 Data Breach Notification guidelines should be maintained.*
3. *Moving to mandatory data breach notification would create a further and significant compliance burden with a corresponding increase in business costs, and business has had more than enough of this already.*

4. *We are not satisfied that there is any compelling evidence that mandatory data breach notification is necessary to achieve the stated goals.*

Avant suggests that continuing and further education to ensure the proactive maintenance of privacy is preferable to a scheme that requires an organisation or individual to potentially incriminate themselves for a breach of privacy which could then be used as an admission in any investigation by the OAIC involving the breach.

In Avant's view the punitive approach of a mandatory obligation supported by civil penalties is unnecessary where an educative approach can achieve the same goals, and there is no evidence that such an approach has failed to have the desired effect.

We remain of that view in 2016 and refer you to our previous submissions for more detail on the reasons for this position.

Despite this position, and on the assumption that a mandatory data breach notification scheme will be introduced, we provide the following comments on the Exposure Draft *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*.

Key Concern: regulation making power and health information

It is clear from the Regulation Impact Statement that the proposed notification regime is directed primarily at preventing catastrophic data breaches in large organisations that could lead to identity theft, stalking, embarrassment or discrimination. The cost benefit analysis assumes that the regime will apply to large organisations and only in the case of serious breaches.

Our key concern about the Bill relates to the regulation making power under clause 26WB(2) of the Exposure Draft, particularly when coupled with the comment in the Explanatory Memorandum (paragraph 7) that:

> *…the Bill provides for regulations to specify particular situations that may also be serious data breaches even if they do not necessarily reach the threshold of a real risk of serious harm. For example,* ***this could include the release of particularly sensitive information such as health records which may not cause serious harm in every circumstance*** *but should be subject to the highest level of privacy protection.* [emphasis added]

The effect of this is that any privacy breach in which health information was lost, accessed or disclosed in an unauthorised manner would be deemed to be a serious data breach requiring notification even if the threshold test was not met, "regardless of the risk of harm" (as noted in the Explanatory Memorandum at paragraph 28). In this case, there is no need to consider any of the matters outlined in clause 26WB(3).

This will place an enormous regulatory and compliance burden on medical practitioners, who are already required to comply with Commonwealth privacy legislation even though they might be small businesses: organisations that hold health information are not able to take advantage of the small business exemption under privacy legislation.

The definition of "health information" under section 6FA the Privacy Act is broad:

*The following information is **health information** :*

(a) information or an opinion about:

(i) the health, including an illness, disability or injury, (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to the individual; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information;

(b) other personal information collected to provide, or in providing, a health service to an individual;

(c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances;

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

The definition would encompass, for example, information about an appointment time, as well as personal information such as name, address and date of birth.

If unauthorised access to or disclosure of *any* health information were deemed to be a serious data breach, the consequences would be that a medical practice would need to notify the Office of Australian Information Commissioner of a breach in circumstances such as:

- an SMS reminder about an appointment sent to the incorrect mobile phone number
- inadvertently sending test results for a patient to the wrong specialist
- a staff member within a medical practice inadvertently accessing patient A's record when they were intending to access patient B's record.

Medical Practitioners' ethical duties

Medical practitioners have stringent ethical and legal obligations of confidentiality in addition to their statutory obligations under privacy legislation. The duty of confidentiality is a long-standing

and fundamental component of the doctor-patient relationship, and as a result medical practitioners have a heightened awareness of the need to protect the privacy of their patient's information. Medical practitioners' obligations of confidentiality are outlined in the Medical Board of Australia's *Good medical practice: code of conduct for doctors in Australia* ("code of conduct"). Medical practitioners also an obligation under the code of conduct to be open and honest when things go wrong, to ensure that the trust that is at the heart of the doctor-patient relationship is maintained.

Avant's view

At Avant we routinely provide advice to our members about their privacy obligations and how to manage privacy breaches including notifying patients where appropriate and taking remedial steps to lessen the impact. In our experience most privacy breaches involving medical practitioners are minor and single incidents.

It is our strong view that, in the mandatory data breach notification regime, health information should be treated in the same way as other information. To be notified, the breach should reach the threshold of a "serious data breach" as outlined in clause 26WB. We believe that there are sufficient safeguards and protections within the requirement to consider the matters outlined in clause 26WB(3), coupled with medical practitioners' ethical duties, to ensure the appropriate level of protection for health information.

To deem a privacy breach in relation to any health information to be a "serious data breach" would:

- have the unintended consequence that minor breaches would need to be notified to the Office of Australian Information Commissioner (contrary to the intention of the legislation as outlined in the Discussion Paper)
- would increase the risk of doctors and practices experiencing "notification fatigue"
- be an unnecessary administrative cost for businesses that in many instances are small businesses and can least absorb the costs.

For these reasons, we submit that in this legislation:

- the regulation making power be removed
- that health information be treated in the same way as other personal information under the breach notification regime.

Summary

Avant's position is that:

1. a mandatory data breach notification regime is not necessary
2. if however a mandatory data breach notification regime is to be introduced, the regulation making power in clause 26WB should be removed
3. health information should be treated in the same was as any other personal information under the regime
4. only a serious data breach relating to health information that meets the threshold of “real risk of serious harm”, taking into account the factors outlined in clause 26WB(3), should fall within the notification provisions.

We would welcome the opportunity to discuss the issues we have raised in more detail if that would be of assistance to the Department.

Avant Mutual Group

4 March 2016