Avant Position Paper

Mandatory data breach notification legislation

Avant mutual group | Your Advantage

Mandatory data breach notification legislation

Avant and its members take privacy obligations and responsibilities seriously. As well as having a statutory duty of privacy, our members have a professional and ethical obligation of confidentiality to their patients, which is the cornerstone of the doctor-patient relationship.

Avant believes:

- A mandatory data breach notification law is unnecessary.
- That should the proposed mandatory data breach notification law be introduced, health information be treated in the same way as any other personal information. Only serious data breaches that meet the threshold of "real risk of serious harm" should be notified.

August 2016

Background

The *Commonwealth Privacy Act 1988*[1] (Privacy Act) was introduced to protect personal information held by Australian Government agencies and to safeguard the collection and use of tax file numbers. Since its commencement, the *Privacy Act* has undergone a series of amendments, including in December 2000[2] when the law was extended to cover some private sector organisations, including private medical practices.

The *Privacy Act* includes Australian Privacy Principles[3] (APPs), which define standards for organisations on collecting, using and disclosing, keeping secure, providing access to, and correcting personal information

There are 13 APPs:

1. open and transparent management of personal information
2. anonymity and pseudonymity
3. collection of solicited personal information
4. dealing with unsolicited personal information
5. notification of the collection of personal information
6. use or disclosure of personal information
7. direct marketing
8. cross border disclosure of personal information
9. adoption, use or disclosure of government related identifiers
10. quality of personal information
11. security of personal information
12. access to personal information
13. correction of personal information.

Source: Privacy Act 1988 Schedule 1[www.legislation.gov.au/Details/C2016C00278]

Avant mutual group

Protecting patients' confidential information has been an important aspect of the doctor-patient relationship since the days of Hippocrates.

The Medical Board of Australia's Code of Conduct, *Good Medical Practice: A Code of Conduct for Doctors in Australia*,[4] states that patients "have a right to expect that practitioners and their staff will hold information about them in confidence, unless information is required to be released by law or public interest considerations".

Medical practitioners also have professional obligations towards their patients when things go wrong:

"When adverse events occur, you have a responsibility to be open and honest in your communication with your patient, to review what has occurred and to report appropriately." [5]

Medical colleges, including the Royal Australian College of General Practitioners[6], and medical representative groups, including the Australian Medical Association[7], also provide guidelines, recommendations and resources to ensure doctors are aware of their obligations and responsibilities on patient privacy.

In 2008, the Australian Law Reform Commission (ALRC) recommended the introduction of mandatory data breach notification in its report *Your Information: Australian Privacy Law and Practice*[8]. The ALRC described mandatory data breach notification as, "in essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information".

In 2013, the then government introduced a mandatory data breach notification Bill into Parliament. The regime contained in that Bill required serious data breaches, which created a "real risk of serious harm", to be reported. However, ultimately the Bill was not passed, after it lapsed during the life of that Parliament.

In December 2015, the issue was reactivated when the Australian Government released a discussion paper and an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* for public consultation[9].

The Bill's Explanatory Memorandum[10] states: "… 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 Australian Government discussion paper[11] pointed out that currently there is no mandate to make a notification following a data breach, although agencies and organisations can make a voluntary notification to the Office of the Australian Information Commissioner (OAIC) for assistance and advice on mitigating the consequences of a data breach.[12] Mandatory data breach notification is required only in the event of unauthorised access to eHealth information under the *My Health Records Act 2012*.

Avant's experience

Avant is Australia's leading medical defence organisation representing more than 68,000 healthcare practitioners and students. Avant's Medico-legal Advisory Service (MLAS) provides support and advice to members when they encounter medico-legal issues, including breaches of privacy.

Breaches of confidentiality and privacy can have a significant impact on the doctor-patient relationship. Failure of a doctor or medical practice to advise a patient of a serious privacy breach and to mitigate the consequences of that breach can lead to the breakdown of the doctor-patient relationship and associated reputational damage. These consequences provide sufficient reasons for medical practitioners to take their obligations and responsibilities of confidentiality to their patients very seriously.

In Avant's experience, most calls to the MLAS regarding breaches of privacy that occur in medical practice relate to breaches that are minor in nature. However, under the proposed mandatory reporting law these minor breaches, which would not reach the threshold of a real risk of serious harm, may still be subject to mandatory reporting.

Case study 1*

A large medical clinic introduces a reminder system for appointments that includes sending a Short Message Service (SMS) to patients. The clinic has two patients with the same name and an appointment reminder is sent to the wrong patient.

The patient's GP, Dr Maloney, seeks advice from Avant on whether the patient should be told about the breach of confidentiality. Dr Maloney is advised to let the patient know that a reminder was sent to the wrong number and that this was an administrative error.

* This scenario is based on Avant claims experience to date. Certain information has been de-identified to preserve privacy and confidentiality.

Case study 2*

A young woman with suspected multiple sclerosis is referred by her GP to Dr Paris, a neurologist, who orders an MRI scan. After receiving a positive result from the scan, Dr Paris discusses treatment options with the patient and dictates a report to be sent to the patient's GP.

Dr Paris's administrative staff inadvertently sent the report to the wrong GP practice. On opening the letter, staff at the GP practice recognise the error. They alert Dr Paris's office and shred the report.

* This scenario is based on Avant claims experience to date. Certain information has been de-identified to preserve privacy and confidentiality.

Case study 3*

A staff member at a general practice is asked by Dr Shelby to scan tests results for patient A into the patient's medical record. However, the staff member inadvertently opens patient B's medical record and starts work on it before realising his mistake.

* This scenario is based on Avant claims experience to date. Certain information has been de-identified to preserve privacy and confidentiality.

These case studies are examples of inadvertent privacy breaches in medical practices that under the current proposed mandatory data breach notification regime may require notification to the OAIC even though the threshold test ("a real risk of serious harm") would not be met.

Analysis and recommendations

A mandatory data breach notification law should not be introduced

The proposed mandatory data breach notification law is directed primarily at preventing catastrophic data breaches in large organisations that could lead to identity theft, stalking, embarrassment or discrimination. In the Regulation Impact Statement[13] for the proposed legislation, a cost-benefit analysis assumes that the law will apply to large organisations and only in the case of serious breaches.

The Bill's Explanatory Memorandum extracted above, suggests that breaches involving health information may be deemed in the legislation to be serious data breaches, no matter how minor, and even if there is no risk of serious harm to the individual/s concerned.

This means any privacy breach that involves unauthorised loss, access or disclosure of health information would be deemed to be a serious data breach requiring notification, even if it is below the threshold test of the real risk of serious harm. This would place an enormous regulatory and compliance burden on medical practitioners who are already required to comply with federal privacy legislation – they are not covered by the small business exemption under the *Privacy Act*.

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 OAIC, which is contrary to the intention of the legislation as outlined in the government's discussion paper
- 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.

Maintain voluntary data breach notification

There is no current evidence that Australian companies, including medical practices, are not acting responsibly in regards to notifying the OAIC and/or an affected individual of a data breach if there is a real risk of harm to the individual.

It would be onerous to introduce a nationwide mandatory data breach notification system as a result of occasional serious breaches across a wide range of organisations and industries.

In Avant's view, the OAIC's data breach notification guidelines[14] should be maintained in conjunction with continuing and further education to ensure the proactive maintenance of privacy. This is consistent with the OAIC's stated educative approach to privacy compliance.

The OAIC guidelines set out clear explanations of how data breaches occur, how to prevent those breaches and the obligations to keep data secure. They also include explanations of when a breach should be reported and the steps that should be taken when a breach occurs.

To ensure privacy is protected, use of the guidelines in conjunction with ongoing education, provided by organisations such as Avant, is preferable to a scheme that requires an organisation or individual to potentially incriminate themselves. The punitive approach based on a mandatory obligation with civil penalties is not necessary when an educative approach can achieve the same goals.

Compliance burden and increased costs

Avant's members often operate in solo practice or small group practices where the introduction of a mandatory audit and compliance system would be costly and inevitably, be passed onto the public via increased health costs. The compliance burden would include costs associated with privacy audits and staff training.

Considerable resources would be needed by organisations to set up and maintain systems to monitor unauthorised privacy breaches at the specific level outlined in the current Bill.

The Bill also provides no fair way to differentiate between larger and smaller companies in implementing mandatory notification systems and, in most cases, the Australian public would bear the cost of the new compliance systems.

Lack of evidence for mandatory data breach notification

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

There is no evidence that members of the public currently feel disempowered and/or would feel empowered if, for example, a minor data breach notification was reported to the OAIC.

Mandatory data breach notification may also cause an individual harm and/or unnecessary distress and would be unwarranted if the breach was minor and had been corrected with no harm caused to the individual.

There is the potential for the OAIC to be overwhelmed by the volume of notifications if all data breach notifications, no matter how minor or insignificant, are reported. Particularly, as there would be the potential for over-notification due to a fear of sanctions for not doing so.

Avant believes the OAIC's resources could be better spent on an education program rather than a mandatory data notification scheme.

Avant's position

Avant believes a mandatory data breach notification scheme is unnecessary because there are currently sufficient safeguards and protections within the Privacy Act, coupled with medical practitioners' ethical and professional duties, to ensure the appropriate level of protection for health information.

However, if a mandatory data breach notification regime were to be introduced, health information should be treated in the same way as other information. To be notified, the breach should unambiguously reach the threshold of a "serious data breach".

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)
- 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.

Key links

- Avant's detailed guide 'Complying with the new Privacy Act (Cth)' **www.avant.org.au/Campaigns/2013/Complying-with-the-new-Privacy-Act-(Cth)/**
- Avant's factsheet 'Privacy essentials' **www.avant.org.au/Resources/Public/20150903-factsheet-privacy-essentials/**
- Avant's 'Guide to Privacy Reforms' **www.avant.org.au/news/20130211-avant-guide-to-privacy-reforms/**
- Avant's submission to the Serious Data Breach Notification Consultation **www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Avant.pdf**

Further reading

- Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 Regulation Impact Statement **www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-Draft-Regulation-Impact-Statement-Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015.pdf**
- Attorney-General's Department: 'Discussion paper: Mandatory data breach notification' **www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-draft-data-breach-notification-2015-discussion-paper.pdf**

References

1. Federal Register of Legislation: Privacy Act 1988. Available from: www.legislation.gov.au/Series/C2004A03712
2. Federal Register of Legislation: Privacy Amendment (Private Sector) Act 2000. Available from: www.legislation.gov.au/Details/C2004A00748
3. Office of the Australian Information Commissioner: Australian Privacy Principles. Available from: www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
4. Medical Board of Australia; Good Medical Practice: A Code of Conduct For Doctors In Australia; Mar 2014. p. 1– 25. Available from: www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx
5. Ibid.
6. RACGP: Standards for general practices (4th edition) Criterion 4:2:1 Confidentiality and privacy of health information. Melbourne: RACGP; Available from: www.racgp.org.au/your-practice/standards/standards4thedition/practice-management/4-2/confidentiality-and-privacy-of-health-information/
7. Alati J. Privacy and Health Record Resource Handbook for Medical Practitioners in the Private Sector. Canberra, ACT (AU): Australian Medical Association; 2014. p. 1-46. Available from: https://ama.com.au/article/privacy-and-health-record-resource-handbook-medical-practitioners-private-sector
8. Australian Law Reform Commission: For your information: Australian Privacy Law and Practice Report. Barton, ACT (AU). Commonwealth of Australia; Mar 2008. p. 1-833. ALRC Report 108. Available from: www.alrc.gov.au/publications/report-108
9. Attorney-General media release: Consultation Opens on Serious Data Breach Notification Bill; 3 Dec 2015. Available from: www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FourthQuarter/3-December-2015-Consultation-Opens-on-Serious-Data-Breach-Notification-Bill.aspx
10. The Parliament of the Commonwealth of Australia, House of Representatives/The Senate. Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 Explanatory Memorandum.
11. Attorney-General's Department: Discussion paper: Mandatory data breach notification. Dec 2015. Available from: www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-draft-data-breach-notification-2015-discussion-paper.pdf
12. OAIC: Data breach notification – A guide to handling personal information security breaches. Sydney, NSW (AU) Aug 2014. p. 1-49. Available from: www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches
13. Attorney General's Department: Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 Regulation Impact Statement. Available from: www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-Draft-Regulation-Impact-Statement-Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015.pdf
14. OAIC: Data breach notification – A guide to handling personal information security breaches. Sydney, NSW (AU) Aug 2014. p. 1-49. Available from: www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

Contact us

New South Wales

Level 28, HSBC Centre, 580 George Street
Sydney NSW 2000
PO Box 746 Queen Victoria Building NSW 1230
Telephone 02 9260 9000 Fax 02 9261 2921

Queensland

Level 11, 100 Wickham Street
Fortitude Valley QLD 4006
GPO Box 5252 Brisbane QLD 4001
Telephone 07 3309 6800 Fax 07 3309 6850

South Australia

Level 1, 195 Melbourne Street
North Adelaide SA 5006
GPO Box 1263 Adelaide SA 5001
Telephone 08 7071 9800 Fax 08 7071 5250

Tasmania

Suite 4, 147 Davey Street
Hobart TAS 7000
PO Box 895 Hobart TAS 7001
Telephone 03 6223 5400 Fax 1800 228 268

Victoria

Level 2, 543 Bridge Road
Richmond VIC 3121
PO Box 1019 Richmond North VIC 3121
Telephone 03 9026 5900 Fax 03 8673 5015

Western Australia

Level 1, 91 Havelock Street
West Perth WA 6005
PO Box 950 West Perth WA 6872
Telephone 08 6189 5700 Fax 08 6189 5713

1800 128 268 **avant.org.au**

3939 08/16 (0567i)

Avant mutual group Your Advantage