27 October 2015

Avant Mutual Group Limited
ABN 58 123 154 898

Registered Office
Level 28 HSBC Centre
580 George Street Sydney NSW 2000

PO Box 746 Queen Victoria Building
Sydney NSW 1230

DX 11583 Sydney Downtown

www.avant.org.au

Telephone 02 9260 9000 Fax 02 9261 2921
Freecall 1800 128 268 Freefax 1800 228 268

OAIC Consultation on Health Privacy Guidance
Office of the Australian Information Commissioner
GPO Box
Sydney NSW 2001

By email: consultation@oaic.gov.au

OAIC health privacy resources

Avant welcomes the opportunity to provide input into the Office of the Australian Information Commissioner's (OAIC) consultation on new draft health privacy resources for private sector health service providers and consumers.

The resources are comprehensive. They will be extremely useful to us in advising our members about their privacy obligations, and to our members in understanding how to comply with their privacy obligations in practice.

Our comments on the resources are attached. There are some sections of the resources such as the resource relating to change of business circumstances that recommend a process that will impose a significant administrative burden on practitioners.

Once you have considered our comments, we would like to arrange to meet with the OAIC to discuss workable solutions to the issues we have raised. Please contact me on the details below to arrange a convenient time to meet.

Yours sincerely

Georgie Haysom
Head of Advocacy

Direct: (02) 9260 9185
Email: georgie.haysom@avant.org.au

About Avant

Avant Mutual Group Limited ("Avant") is Australia's largest medical defence organisation, and offers a range of insurance products and expert legal advice and assistance to over 64,000 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.

Avant submissions on the OAIC draft health privacy resources

General comments

Avant commends the OAIC on producing these comprehensive resources. .

The resources for health service providers will be extremely useful to us in advising our members about their privacy obligations, and to our members in understanding how to comply with their privacy obligations in practice. The references to other jurisdictions that have privacy legislation, case examples and additional compliance tips throughout the 11 business resources are particularly useful. However, there are specific issues that we consider require further clarification as discussed below.

Responses to selected business resources

Business resource: Handling health information under the Privacy Act: a general overview for private sector health service providers

The *Health Legislation Amendment (eHealth) Bill* 2015 (the Bill) introduced on 17 September 2015 and passed by the House of Representatives on 15 October 2015 will amend the *Personally Controlled Electronic Health Records (PCEHR) Act* 2012. One major amendment is to the name of the Personally Controlled Electronic Health Record (PCEHR) to "My Health Record", and the PCEHR Act to the *My Health Records Act* (the Act). In the event that the Bill is also passed by the Senate, we recommend updating sections within this business resource to reflect the system name change to the My Health Record system (previously known as the PCEHR system).

Under the amending legislation, as part of measures to reduce the regulatory burden on healthcare provider organisations, the registration process for the My Health Record system will be simplified and the need to enter into participation agreements will be removed from the Act. Therefore, we recommend removing references to participation agreements in this business resource.

In the event that the Bill is passed by the Senate, Avant recommends updating the following section to reflect these changes:

> **My Health Record ~~PCEHR~~ system**
>
> If you participate in the My Health Record system ~~Personally controlled electronic health record system~~, you must also comply with the *My Health Records Act* ~~*Personally Controlled Electronic Health Records Act*~~ *2012* and *Healthcare Identifiers Act 2010*, and their accompanying Rules and Regulations.~~, and other requirements contained in your participation agreement with the System Operator.~~

The Act will require all entities to report data breaches in certain circumstances to the My Health Record System Operator and/or the Australian Information Commissioner. Currently, registered healthcare provider organisations and registered contracted

service providers are not subject to this requirement but are instead obliged through contractual arrangements to report data breaches.

In the event that the Bill is passed by the Senate, we recommend updating the following sections to reflect these changes:

> **Data security (APP 11)**
>
> If you participate in the My Health Record ~~personally controlled electronic health record~~ system, you will also have ~~contractual~~ statutory obligations to notify the System Operator of data breaches in certain circumstances.
>
> **What could happen if I breach the APPs?**
>
> **…**
>
> If you participate in the My Health Record ~~personally controlled electronic health record~~ system, you will also have ~~contractual~~ statutory obligations to notify the System Operator of data breaches in certain circumstances.

Avant has previously recommended that the OAIC include a reference to state and territory legislation and the general law regarding use and disclosure of information relating to deceased persons. We are pleased to see that the OAIC has included this information in a compliance tip within this business resource.

Business resource: Key health privacy concepts

The section entitled "Permitted health situations and permitted general situations" is confusing because of the use of the word "permitted" and "exceptions" in the same paragraph. Although there is more detail later in the series, it would be helpful to have an example in this section to illustrate the practical effect of these exceptions.

Business resource: Collecting patients' health information

Mutual trust and building rapport are fundamental principles of the doctor-patient relationship. Doctors cannot generally provide proper, ongoing care to patients in an anonymous relationship. Further, medical records are created to facilitate continuity of care between different healthcare practitioners and healthcare organisations. This is extremely difficult to achieve where a patient's information is anonymised with the risk of harm to a patient if the correct and appropriate information is not available.

Avant believes it would rarely be practical to provide patients with the option of not identifying themselves, or of using a pseudonym. A good example of this is when treating patients with sexually transmitted infections (STIs). Further, where pathology, radiology, medication or referral is required it will be almost impossible to provide care to an anonymous patient or a patient who chooses to use a pseudonym. Treating patients anonymously raises clinical, ethical and medico-legal risk issues.

We are pleased that the section "Anonymity and pseudonymity" allows an exception to treating patients anonymously. However, we believe the OAIC should mention that it is unlikely that health professionals would be expected to treat patients anonymously.

This reference to anonymity not being a practical consideration in medical practice is also relevant and should be included in the section "Patients who wish to be anonymous or use a pseudonym (APP 2)" in the *Business resource: Handling health information under the Privacy Act: A general overview for health service providers* and in the section "Can you use a health service anonymously" section in the consumer focused *Fact sheet: Privacy and your health information*.

We recommend this business resource link to the section "Laws requiring or authorising use or disclosure" in the *Business resource: Using and disclosing patients' health information* as STIs are a communicable and often notifiable disease and dealing with anonymity may be impractical.

Business resource: Using and disclosing health information to provide a health service

Avant recommends including the "provision of legal advice" as a directly related purpose in the following section:

> **Directly related purpose**
>
> Other directly related purposes include many activities or processes necessary for the functioning of the health sector. Provided these purposes fall within the individual's reasonable expectations, no additional steps need be taken before using or disclosing the information in this way. These purposes may include:
>
> …
>
> - disclosure to a medical expert (only for medico-legal opinion), an insurer, a medical defence organisation, or a lawyer, solely for the purpose of addressing liability indemnity arrangements (such as reporting an adverse incident), ~~or~~ for the defence of anticipated or existing legal proceedings, or for the provision of legal advice.

In relation to the section "Sharing information with other health service providers without consent", we recommend that the following paragraph is amended to read as set out below to clarify the obligations:

> **Sharing information with other health service providers without consent**
>
> …
>
> If a patient's information is likely to be shared within a treating team, you should tell the patient that such disclosures may take place. Where practicable you should also tell the patient who ~~is in~~ may be in the treating team (such as a GP, physician, physiotherapist and others), and ~~how much~~ the type of information that may be disclosed to particular members of the team. A patient may be sensitive about certain information being shared

without their consent even across a treatment team, or with particular members of it but it may need to be disclosed in order to treat the patient appropriately.

Business resource: Access to health information held by health service providers

This business resource states that the "APPs do not require access requests to be made in writing". However, section 26 of the *Health Records and Information Privacy Act 2002* (NSW) states that a request "…must be in writing". We therefore recommend that this part of the business resource is amended to refer to the state based statutory provisions and clarify what provisions healthcare providers are required to follow. Likewise, under the section dealing with "responding to access requests" it states that a "reasonable period will be 30 calendar days or less". By contrast the NSW Act specifies in section 27 that requests are to be responded to within "45 days after receiving the request".

The Medical Board of Australia's Guidelines: Technology-based patient consultations outline that doctors must "make a judgement about the appropriateness of a technology-based patient consultation and in particular, whether a direct physical examination is necessary". Providing access to personal information over the phone may not always be clinically appropriate.

Avant is pleased that the following section only requires doctors to comply with giving access over the phone if it is reasonable and practicable to do so.

We would recommend acknowledging the limitations of disclosing information over the phone by including the following amendment:

Giving access

Access to personal information can be provided in a variety of ways, such as:

…

- giving the information over the phone or by email, for example test results where clinically appropriate

…

Business resource: Correction of health information by health service providers

This business resource states that reasonable steps to correct personal information could include making appropriate "…deletions" of information.

In New South Wales, alteration of medical records by deletion is not permitted as set out in clause 4 of Schedule 2 of the *Health Practitioner Regulation (NSW) Regulation* 2010, which states:

4 Alteration and correction of records

A medical practitioner or medical corporation must not alter a record, or cause or permit another person to alter a record, in a way that obliterates,

obscures or renders illegible information that is already contained in the record

Avant recommends including a reference to this provision in the following paragraph:

Reasonable steps to correct personal information

…

Reasonable steps to correct personal information could include making appropriate additions, deletions or alterations to information, or not correcting the information if it would be unreasonable or unlawful to do so. In some cases, it may be appropriate to destroy or de-identify the information (see information that is 'Out-of-date' above). In NSW, for example, a medical practitioner or medical corporation must not alter a record in a way that obliterates, obscures or renders illegible information that is already contained in the record.

We recommend that this provision also be referred to in the compliance tip on page 4 of this business resource.

The reference to correction and alteration of medical records in NSW is also relevant to the section "Quality and correction of personal information (APPs 10 and 13)" in the *Business resource: Handling health information under the Privacy Act: A general overview for health service providers* and similar amendments should be made to the section "Correcting your health information" in the consumer focused *Fact sheet: How you can access or correct your health information*.

The OAIC uses "coeliac disease" as an example of misleading information in a medical record. Avant recommends using a different example as this may imply that a reasonably formed opinion (or differential diagnosis) at one point in time is considered misleading and should therefore not be recorded in the medical record, or should be corrected at a later point in time. We consider that this is not good practice and may increase the medico-legal risk of doctors and the risk of harm to patients.

The commentary refers practitioners to "associate a statement with their record" when they have refused to correct information. We presume it means that a practitioner is required to note that the patient has asked them to correct a particular part of the record, that they have refused and the basis for refusal. Avant recommends rewording this sentence to clarify what practitioners must do in this situation.

Avant recommends providing a case example in the section entitled "What to do when refusing to correct information".

Business resource: Collecting, using and disclosing health information for health management activities

We believe is it unclear how the section "Reasonable steps to de-identify the information before disclosure" would apply in practice. There are many instances in practice where information is collected for business management purposes and then

has to be disclosed for business management purposes, and this cannot be done in a de-identified manner. For example, practices engage debt collection agencies to recoup unpaid fees and this necessarily involves disclosure of identifiable patient information.

We therefore recommend including a case example of when and how a practitioner would need to de-identify information in the section entitled "Reasonable steps to de-identify the information before disclosure".

Business resource: Disclosure of health information and impaired capacity

Avant agrees that in assessing capacity of an individual under the age of 18, factors to be considered by the doctor include the maturity of the young person and the capacity to understand and appreciate what is being proposed. However, the basis upon which the OAIC has chosen 15 as the age of presumed capacity is unclear.

In our experience the age of 14 is a better guide for capacity and is consistent with Medicare rules and other legislation such as the *Minors (Property and Contracts) Act 1970* (NSW).

For example, Medicare's policy on access to records of an individual under 14 years of age in the "Request for Medicare and PBS claims information for individuals and families form" states that:

> *A person with parental responsibility can generally get Medicare or PBS information about a child where the child is under 14 years of age and listed on the same Medicare card as the requesting person.*

Avant believes it is too restrictive to indicate that is appropriate to presume capacity from age 15. It is more reasonable to presume that a patient aged under 14 years does not have the capacity to give consent.

Avant recommends amending the following example accordingly:

> **Example: Do children have the capacity to legally give consent?**
>
> The Privacy Act does not specify an age after which individuals can make their own privacy decisions. Generally, an individual under the age of 18 has capacity to consent where they have a sufficient understanding and maturity to understand what is being proposed. This determination will require an assessment on a case by case basis.
>
> If it is unreasonable or impracticable to assess capacity, you may presume that a patient aged under 14 ~~15~~ years does not have the capacity to give consent. In these circumstances, you may disclose their health information to a person responsible for the child such as the child's parent or guardian in the circumstances outlined in this exception.

The OAIC has made an important point about the difference between consent for handling health information and consent for treatment in *Business resource: Collecting patients' health information*.

Avant recommends including the relevant extract from the section "Obtain consent before collecting health information" in the *Business resource: Collecting patients' health information* within the following section:

> **Disclosure to a responsible person for the patient**
>
> You can only disclose a patient's health information to a 'responsible person' for the patient.
>
> …
>
> Consent, as discussed in the Business resource: Collecting patients' health information, applies to decisions about how a patient's health information is handled. It does not cover consent to receive treatment. In practice, consent to the handling of health information and consent to treatment often occur at the same time, though they are distinct authorities by an individual to do different things: to provide treatment *and* to handle health information in particular ways.

Avant recommends including a statement in the section "Disclosure to a responsible person for the patient" referring to state and territory legislation about the appropriate substitute decision-maker for treatment decisions, as these may be different from the responsible person under the Privacy Act.

Business resource: Change of business circumstances or closure of a health service

This business resource states that old and new health service providers are required to obtain "…each patient's consent" before ownership of medical records can be transferred following a sale of a health practice.

Avant strongly believes that this is impracticable. Imposing requirements on new health service providers (when there is a change in business circumstances) to obtain each patient's consent to collect information (regardless of whether or not the new health service provider will use or disclose the information for new purposes) will place a considerable cost and administrative burden on practitioners. Due to the legislative requirement to retain medical records, practices often hold thousands of records dating back numerous years – in the case of children up to 25 years. It is an excessive burden and often not possible to contact each of these patients to consent to the transfer of their records. In the event that consent cannot be obtained it will mean that the old health service provider has to retain the medical records in storage after he has retired or moved to another state/ practice.

In NSW the requirement to retain medical records is complied with by transferring medical records to another medical practitioner without the need to obtain consent from individual patients (*Health Practitioner Regulation (NSW) Regulations* – Regulation 11).

As the holder of health information, the new health service provider will be subject to the same legal and ethical requirements concerning medical records as the old health service provider. Patients retain their right of access to health information at the new practice.

We note the following paragraph from the *Business resource: Using and disclosing patients' health information:*

> The Privacy Act is not intended to impose unnecessary administrative burdens on providers, or to inconvenience patients, by requiring consent every time health information is appropriately shared with another provider, or otherwise handled in the delivery of healthcare. At the same time, the Privacy Act seeks to ensure that individuals retain appropriate control over how their information is handled, including ensuring that it is not handled in ways that an individual would not expect.

These comments apply equally to this business resource. We believe that the individual's right to know how their information is handled upon the sale of the business can be addressed appropriately in the practice's privacy policy under APP 1.

Avant would welcome the opportunity to provide you with practical examples of the difficulties practices will face in complying with the *Business resource: Change in business circumstances for a health service provider*, and explore a more practical solution to this issue.

The section on 'data quality' implies that a health care provider who is transferring records to a new provider should undertake a data cleansing process before the transfer. This will be a costly, impractical and time consuming process for practitioners.

Avant contact details

Should you have any further queries in relation to this submission, please contact:

Georgie Haysom

Head of Advocacy, Avant

Telephone: 02 9260 9185

Email: Georgie.haysom@avant.org.au

27 October 2015