



Our Ref: KM:300726

3 November 2021

TO: AUSTRALIAN PHYSIOTHERAPY ASSOCIATION

ATTN: ANJA NIKOLIC **EMAIL:** Anja.Nikolic@australian.physio

FROM: Kristy Muhlhan

ADVICE: COVID 19 MANDATORY VACCINATIONS AND ENTERING PREMISES – NATIONAL

We refer to previous correspondence.

The following advice is current as at today's date, 3 November 2021, but continues to change as a result of public health orders in place in each Australian jurisdiction.

The purpose of this email is to advise you further, on the following:

1. Current public health orders in place in each Australian jurisdiction; and
2. Privacy obligations regarding vaccination information of patients;
3. Whether business owners (particularly, physiotherapists) can refuse entry and treatment to an unvaccinated person and the risks involved.

This advice is not intended to extend to privacy obligations or risks from an employer/employee perspective.

1. PUBLIC HEALTH ORDERS

- 1.1. The most up-to-date directions for each jurisdiction may be found at the following links:

Jurisdiction	Public health orders or directions
Queensland	Chief Health Officer public health directions
New South Wales	COVID-related legislation: Public health orders
Australian Capital Territory	ACT Public Health Directions
Victoria	Directions issued by Victoria's Chief Health Officer
South Australia	Emergency Declaration and Directions

Western Australia	COVID-19 coronavirus: State of Emergency Declarations
Tasmania	Coronavirus disease (COVID-19): Resources
Northern Territory	Chief Health Officer Directions

1.2. As the directions are extensive, we do not intend to summarise them, save to say that there are currently no directions in place across any of the Australian jurisdictions that require mandatory vaccination for patients and/or visitors (but expressly excluding workers) to attend healthcare premises. We note the following directions of particular relevance:

1.2.1. **Victoria:** [Open Premises Directions \(No 3\)](#) require that 'open premises' only allow fully vaccinated persons or an excepted person into their premises. The list of 'open premises' are detailed in Column 1 of Schedule 1 to the abovementioned directions. A medical centre (including an allied health practice) does not fall within the definition of open premises.

1.2.2. **New South Wales:** [Public Health \(COVID-19 General\) Order 2021](#) and [Public Health \(COVID-19 General\) Order \(No 7\) 2021](#) generally provides that premises must remain closed to unvaccinated adults in certain circumstances. However, a 'medical centre' (which includes allied health professionals) does not fall within the definition of 'retail premises' nor does it fall within the definition of 'business premises' or any of the other types of premises listed at Division 5, Part 2 of [Public Health \(COVID-19 General\) Order 2021](#) or at Schedule 1 of [Public Health \(COVID-19 General\) Order \(No 7\) 2021](#). However, please note that a shop that sells medical or pharmaceutical supplies is considered a 'retail premises', but still remain exempt to the relevant direction as they are considered 'critical retail premises'.

1.3. The scope of this advice does not include considering whether the public health orders in each jurisdiction in Australia is lawful and, if so, the legal framework that governs the public health orders.

2. PRIVACY OBLIGATIONS – PERSONAL INFORMATION AND VACCINATION STATUS

2.1. The following advice applies to all jurisdictions in Australia.

2.2. The *Privacy Act 1988 (Cth)* deals with the rights of organisations and agencies to handle an individual's personal information (including sensitive information) and privacy rights.

2.3. Despite the fast-moving nature of issues relating to COVID-19, businesses must still comply with their obligations under applicable privacy laws and including the Australian Privacy Principles and the Notifiable Data Breaches scheme.

-
- 2.4. The Australian Privacy Principles (“APPs”) cover the collection, use, disclosure and storage of personal information. They apply to various businesses and organisations and include private businesses with an annual turnover of more than \$3 million and small business operators with a turnover of less than \$3 million in certain circumstances, which includes private sector health service providers and including allied health professionals. A summary of the APPs is set out as a Schedule to this email.
- 2.5. The Notifiable Data Breaches scheme requires that an organisation or agency governed by the *Privacy Act* must notify affected individuals and the Office of the Australian Information Commissioner (“OAIC”) where a data breach is likely to result in serious harm to an individual whose personal information is involved, for example, where personal information is lost or subjected to unauthorised access or disclosure.
- 2.6. ‘Personal information’ under the *Privacy Act* is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not that information is true or not and whether or not it is recorded in a material form. For example, a person’s name, address, email address, telephone number, date of birth, signature, bank account details, **health information** or any commentary or opinion about a person. It also includes data relating to a person that has been collected or generated through the operation of the COVIDSafe app. This would also include, for example, collecting personal information for the purpose of contact tracing, which we have detailed further below.
- 2.7. ‘Sensitive information’ under the *Privacy Act* attracts a higher level of protection. It includes various information about an individual’s race, political opinions, religious beliefs, sexual orientation, criminal record and **health and genetic information**. This includes for example, vaccination status of patients.
- 2.8. Sensitive information should only be handled by organisations in the following ways:
- 2.8.1. ‘sensitive information’ may only be collected with consent, except in specified circumstances. Consent is generally not required to collect ‘personal information’ that is not ‘sensitive information’;
- 2.8.2. ‘sensitive information’ must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;
- 2.8.3. ‘sensitive information’ cannot be used for the secondary purpose of direct marketing; and
- 2.8.4. ‘sensitive information’ cannot be shared by ‘related bodies corporate’ in the same way that they may share other ‘personal information’.
- 2.9. **Collection and disclosure of COVID-19 vaccination status of patients/visitors**
- 2.9.1. Australian Privacy Principle 3 (collection of solicited personal information) sets out the circumstances when an organisation may collect personal information. Uplifted privacy protections apply to a person’s COVID-

19 vaccination status since it constitutes health information and is therefore 'sensitive information' for the purpose of the *Privacy Act*.

2.9.2. The collection of the sensitive information must be reasonably necessary for the business' functions and activities (which may include preventing or managing the transmission of COVID-19 in the workplace). The following factors may be relevant to whether the collection of COVID-19 vaccination status information would be considered reasonably necessary for a business' activities or functions:

2.9.2.1. current public health advice for the prevention or management of COVID-19;

2.9.2.2. health and safety risks in the business' work sector;

2.9.2.3. applicable workplace laws; and

2.9.2.4. obligations under contracts.

2.9.3. Service providers must be transparent with patients/visitors about the reasons for collecting and disclosing COVID-19 vaccination status information including that collection must comply with Australian Privacy Principle 5 (notification of the collection of personal information) and including the following:

2.9.3.1. the entity's identity and contact details;

2.9.3.2. the fact and circumstances of collection;

2.9.3.3. whether the collection is required or authorised by law;

2.9.3.4. the purposes of collection;

2.9.3.5. the consequences if personal information is not collected;

2.9.3.6. the entity's usual disclosures of personal information of the kind collected by the entity;

2.9.3.7. information about the entity's Privacy Policy;

2.9.3.8. whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

2.9.4. Only the minimum amount of personal information reasonably necessary to maintain a safe workplace should be collected, used or disclosed by a service provider.

2.9.5. We recommend that:

2.9.5.1. COVID-19 vaccination status information should be used or disclosed on a need-to-know basis.

- 2.9.5.2. Service providers should ensure that they take reasonable steps to keep patient/visitor COVID-19 vaccination status and related health information secure.
- 2.9.5.3. As a matter of best privacy practice, service providers should be mindful of the sensitive nature of the health information of patients/visitors in relation to the collection, storage, use and disclosure of COVID-19 vaccination status and regularly review whether there is a need to retain this information.

2.10. Collection of personal information and contact tracing

- 2.10.1. The OAIC has published guidance material to assist businesses in understanding their obligations when collecting personal information about customers and visitors to their premises for the purpose of COVID-19 contact tracing.
- 2.10.2. In summary, the OAIC notes that where businesses **are required** to collect “contact information” under the terms of “orders or directions” the businesses should:
 - 2.10.2.1. Limit the collection of personal information to that which is required under the relevant public health order;
 - 2.10.2.2. Notify individuals before collecting personal information, to satisfy requirements under Australian Privacy Principle 5 (as discussed at paragraph 2.8.3 above). This can also be achieved by displaying a prominent notice on their premises and website, and reinforcing the information when speaking with patients or visitors;
 - 2.10.2.3. Store the information securely once it has been collected, while also taking care to observe obligations under the notifiable data breaches scheme;
 - 2.10.2.4. Disclose the information to relevant health authorities involving in contact tracing activities upon the requirement of those authorities;
 - 2.10.2.5. Destroy the information if it is no longer reasonably necessary for the purposes of contact tracing. A public health order may specify a period for which the information must be retained. If no period is specified, the OAIC guides that information should be destroyed after a reasonable period, which would usually be within 28 days.
- 2.10.3. Where businesses are **not required** to ask for customer names and contact details for contact tracing purposes under a public health order, those businesses may still collect contact information where doing so would be a normal part of the businesses’ functions and activities (e.g. booking appointments).

2.10.4. Depending on the jurisdiction in Australia, some businesses will have record keeping obligations under the relevant public health orders.

3. REFUSAL OF ENTRY AND TREATMENT TO UNVACCINATED PERSONS

3.1. Is it mandatory for visitors to be vaccinated?

3.1.1. No, it is not mandatory in any State or Territory of Australia for persons entering a healthcare setting to be vaccinated.

3.2. Can a healthcare service provider require visitors to be vaccinated?

3.2.1. *Discrimination*

3.2.1.1. In Australia, it is unlawful to discriminate on the basis of a number of protected attributes.

3.2.1.2. Each State and Territory in Australia also has enacted anti-discrimination legislation. For the purpose of this advice, we do not propose addressing those laws individually and provide general advice only. In the event that you require advice specific to an allied health practice, we recommend a full review and advice including on discrimination laws that are relevant to the particular jurisdiction.

3.2.1.3. Whilst there are differences between the legislation concerning discrimination laws across the jurisdictions, all legislation dealing with discrimination contains a similar framework for identifying unlawful discrimination. Generally, for discrimination to be unlawful, an act or omission must:

3.2.1.3.1. Be based on one of the grounds or attributes set out in the legislation, for example, disability, race, sex or age;

3.2.1.3.2. Result in harm, less favourable treatment or disadvantage whether direct or indirect discrimination;

3.2.1.3.3. Fall within an area of activity set out in the legislation, such as employment, education or the provision of goods or services;

3.2.1.3.4. Not fall within an exception, exemption or defence.

3.2.1.4. Put simply, you cannot discriminate in the provision of goods and services (including healthcare services) based on protected attributes.

3.2.1.5. Where a service provider requires all patients/visitors to be vaccinated, refusal of entry may amount to discrimination, depending on the particular circumstances.

-
- 3.2.1.6. There may be defences available to the service provider for example, in Victoria the defence of 'statutory authority' may be available in circumstances where a vaccination requirement is authorised under health and safety laws which require organisations to provide a safe working environment for staff and customers. However, there would also be limitations to such a defence where an exception is not made, for example, someone with a medical condition or disability may prevent them from getting a vaccination. This could amount to indirect discrimination or failure to make reasonable adjustments.
- 3.2.1.7. If however the person's reason for not wanting the vaccine is not linked to a protected attribute under the relevant discrimination laws, then it is unlikely that this would amount to discrimination (although this would need to be assessed based on the particular circumstances). For example, if the reason for not getting the vaccine is due to a personal preference or concerns about side effects.
- 3.2.1.8. Where it is reasonably necessary to protect the health and safety of any person or the public generally, discrimination may be allowed under the discrimination laws. For example, in Victoria, the *Equal Opportunities Act* allows this but only on the basis of disability or physical features. Therefore, if the service provider wishes to make vaccination a mandatory requirement, they must prove how this health and safety exception applies. Health and safety grounds are likely to be relevant to other attributes as well because of the defences available and the requirements in workplace health and safety laws to provide a safe environment for customers as far as is reasonable practicable.
- 3.2.1.9. Matters that may be relevant to considering whether it is reasonably practicable to require patients/visitors to be vaccinated include:
- 3.2.1.9.1. the type of service provided and the people that access it, and whether there is a heightened risk they will suffer severe symptoms if they contract COVID-19 (for example, care or support service settings where there are people over 60 or medical goods for people with pre-existing health conditions);
 - 3.2.1.9.2. the physical space of the location (where the clinic is located) and associated risk of transmission;
 - 3.2.1.9.3. whether alternative measures could have been put in place to protect employees and any members of the public who enter the location (COVIDSafe Plan or other control measures);

- 3.2.1.9.4. the rate of community transmission at the time;
- 3.2.1.9.5. the availability of the vaccine;
- 3.2.1.9.6. advice from workplace health and safety bodies about vaccinations at the time (for example, WorkSafe Victoria).
- 3.2.1.10. While a defence to a claim of indirect discrimination is that it was reasonable for the business to mandate COVID-19 vaccinations, success in this defence will be highly dependent on the facts of the case.
- 3.2.1.11. Where there is not an explicit law requiring that a person be vaccinated, service providers should be very cautious about imposing mandatory COVID-19 vaccination policies or conditions on patients/visitors, particularly in a healthcare setting and we do not recommend it. Refer to our further comments below at paragraph 3.3.

3.2.2. **Human Rights**

- 3.2.2.1. Within Australia, the Australian Government have particular responsibilities to ensure that human rights are protected. Our system of human rights is found in the Australian Constitution as well as legislation and common (Court made) law.
- 3.2.2.2. The laws concerning human rights continue to apply even during the COVID-19 pandemic. The scope of our advice does not include addressing the human rights law relevant to each jurisdiction in Australia. However, as a guide, human rights include such matters as the right to equality and to be protected from discrimination, the right not to be subjected to medical or scientific treatment and the right not to have privacy interfered with.
- 3.2.2.3. However, human rights are not absolute and can be limited in some circumstances. Any limitation on rights must only go so far as necessary to achieve a legitimate purpose and, if limiting a right is necessary, the action taken should be reasonably justified and proportionate, and the least restrictive means available.

3.3. **Vaccination Policy**

- 3.3.1. A vaccination policy of a service provider is separate to any public health order and must be carefully considered.
- 3.3.2. A service provider cannot force a patient or visitor to be vaccinated.
- 3.3.3. A mandatory COVID-19 vaccination policy does not force a patient or visitor to be vaccinated but, rather, it outlines the standard the service

provider requires for patients/visitors to enter a premises and could underpin several objectives held by the service provider, including addressing health and safety obligations for staff in the workplace and others attending the premises and safeguarding its reputation.

- 3.3.4. A mandatory COVID-19 vaccination policy may, for example, prevent unvaccinated persons from entering the premises, limit or restrict access or require alternate means for reducing the risk of COVID-19 transmission (e.g. rapid antigen test).
- 3.3.5. Where service providers are not the subject of the mandatory vaccination requirements imposed by public health orders, this question involves weighing up whether the requirement of a service provider for patients and visitors to be vaccinated to enter the premises is lawful, not discriminatory and reasonable for the health and safety of its workers.
- 3.3.6. Whilst the Federal Government arguably has the power to legislate on mandatory vaccination, the Prime Minister has made clear that it has no intention of passing any special laws in respect of mandatory vaccination and instead the onus is on the state governments under the state of emergency powers and requiring businesses to consider further whether to seek to deny access to a premise or a service based on whether people are vaccinated or non-vaccinated against COVID-19.

3.4. Health & Safety

- 3.4.1. Businesses have health and safety obligations to their workers and other persons in their workplace, including during an infectious disease outbreak like COVID-19.
- 3.4.2. Businesses have a duty to eliminate, or if that is not possible, to minimise so far as is reasonably practicable, the risk of exposure to COVID-19 in the workplace under workplace health and safety laws.
- 3.4.3. Whilst mandatory COVID-19 vaccination is a decision that a business needs to make considering the circumstances of their workplace, most businesses will not need to make vaccination mandatory to comply with their statutory workplace health and safety obligations. Ultimately, whether a business requires workers or persons attending the workplace to be vaccinated will depend on the particular circumstances arising from a 'risk assessment' by the business with reference to the nature of their business and the current public health orders in effect.

3.5. Therapeutic Goods Administration ("TGA")

- 3.5.1. The TGA is the body that regulates the advertising of therapeutic goods in Australia, including COVID-19 vaccinations.
- 3.5.2. **Any communication that seeks to promote COVID-19 vaccination, including service provider COVID-19 vaccination policies or communications encouraging vaccination, are subject to the TGA's regulations.**

- 3.5.3. The TGA has provided certain permissions and guidance on how certain entities can lawfully provide communications about COVID-19 vaccines to support the government's roll-out strategy. Put simply, any communication must be consistent with current Commonwealth government health messaging regarding the national COVID-19 vaccination programme and must not contain:
- 3.5.3.1. Any reference to the trade name, sponsor or active ingredient or any other information that would identify the vaccine e.g. Pfizer, AstraZeneca, except where approved by the vaccination provider;
 - 3.5.3.2. Any statement, or implication comparing different COVID-19 vaccines (or comparing vaccines with treatments such as medicines);
 - 3.5.3.3. Any statements to the effect that COVID-19 cannot cause harm or have no side effects;
 - 3.5.3.4. Any statement regarding COVID-19 vaccines that is false or misleading.

4. CONCLUSION

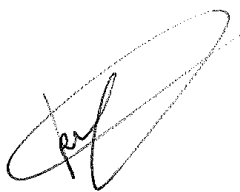
4.1. In summary:

- 4.1.1. Vaccination is free and voluntary, unless a state or territory public health order (or other law) is in place or, a business implements a mandatory vaccination policy for persons entering their workplace premises;
- 4.1.2. Public health orders are creating a clear divide between what the vaccinated and unvaccinated are allowed to do, but this does not extend to accessing healthcare services;
- 4.1.3. The public health orders seem set to disappear over time when emergency powers come to an end, leaving businesses to make their own calls on how they run their operations;
- 4.1.4. If a healthcare provider is considering mandating a vaccination policy within their workplace for patients and/or visitors, we caution them against it and we do not recommend it without careful consideration and a risk assessment, which should only be done on a case-by-case basis considering a business' particular circumstances, the laws relevant to the jurisdiction and the reasons why they wish to implement it;
- 4.1.5. Where patients/visitors co-operate and freely and voluntarily consent and provide their vaccination information to a service provider, this should not affect their operations. However, where patients/visitors exercise their privacy rights not to disclose such information, service providers will need to consider their COVIDSafe Plan which may include alternate control measures to be implemented in their business (such as rapid antigen testing, restricted access to the workplace premises, restricted access to particular workers etc.);

-
- 4.1.6. We do not recommend patients be turned away and refused treatment based on their vaccination status, as this may have indirect discrimination implications, depending on the individual's personal circumstances;
- 4.2. In terms of practical steps, we strongly recommend each service provider have in place:
- 4.2.1. COVIDSafe Plan – this may not be required in all jurisdictions but we encourage business's and organisations to have a COVIDSafe Plan (or similar) in place, irrespective of the public health orders / Government directions in place;
- 4.2.2. Privacy Policy – this is a policy that explains in simply language how an organisation or business handles personal information (including vaccination information);
- 4.2.3. Business Continuity Plan – this is a document that outlines how a business will continue to operate during an unplanned disruption in service for example, as a result of a COVID outbreak in your premises.
- 4.3. It is also strongly encouraged as a risk management strategy, that businesses adopt the principles for the privacy of personal information contained in the *Privacy Act* when collecting and handling the personal information of workers, patients and visitors and that workers involved in the collection and handling of medical and health information are aware and understand the obligation of confidence and relevant privacy principles. Businesses may wish to undertake an audit of their information handling practices to identify how medical and health information is collected, used and stored.

Thank you as always for your instructions.

Yours faithfully,
BURKE & ASSOCIATES LAWYERS PTY LTD



Kristy Muhlhan
Principal
LL.B (Hons) Grad Dip LP. GAICD
kmuhlhan@burkelawyers.com.au

SCHEDULE - AUSTRALIAN PRIVACY PRINCIPLES SUMMARY

Australian Privacy Principle	Summary
Open and transparent management of personal information	An organisation must take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs, and enable the entity to deal with inquiries and complaints regarding compliance with the APPs. This includes a clearly expressed APP privacy policy.
Anonymity and pseudonymity	Individuals must have the option of not identifying themselves, or using a pseudonym, when dealing with the organisation.
Collection of solicited personal information	<p>An organisation must not collect personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities. Collection of personal information must only be by lawful and fair means. Information must only be collected from the individual (unless an exception applies, such as it is unreasonable and impracticable to do so).</p> <p>Where the personal information is sensitive information, an organisation must not collect the information unless the individual consents (unless an exception applies, such as the collection is authorised by court order).</p>
Dealing with unsolicited personal information	If an organisation receives personal information, and the organisation did not solicit the information, the organisation must make a determination whether it would have been able to solicit the information under APP 3 . If the organisation determines it could not have solicited the information under APP 3 , it must destroy the information or ensure the information is de-identified.
Notification of the collection of personal information	An organisation must take reasonable steps to notify an individual about the collection of personal information, either before or at the time of collection, and if that is not practicable as soon as possible thereafter. APP 5 requires the organisation to notify the individual on a range of matters regarding the collection of their personal information, including the purpose for which the information has been collected, the main consequences (if any) to the individual if the personal information is not collected, and any possible disclosure of the information.
Use or disclosure of personal information	If an organisation holds personal information about an individual that was collected for a particular purpose, the organisation must not use or disclose the information for another purpose. There are exceptions to this rule, including if the individual consents and or if the organisation is required to disclose under a court order.
Direct marketing	If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the

	purpose of direct marketing. There are exceptions of this rule, including with the consent of the individual.
Cross-border disclosure of personal information	Before an organisation discloses personal information about an individual to a person or organisation who is not in Australia, the organisation must take reasonable steps to ensure the overseas recipient of the information does not breach the APPs.
Adoption, use or disclosure of government related identifiers	An organisation must not adopt a government-related identifier as its own identifier. A government-related identifier is an identifier of that individual that has been assigned by a government agency or authority (for instance, a tax file number assigned by the Australian Taxation Officer). There are exceptions to this rule, including where required or authorised under a court order.
Quality of personal information	An organisation must take reasonable steps to ensure that the personal information it collects uses or discloses is accurate, up to date and complete.
Security of personal information	An organisation must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.
Access to personal information	If an organisation holds personal information about an individual, the organisation must, on the individual's request, give the individual access to the information. There are exceptions to this rule, including if the organisation believes that giving access would pose a serious threat to the life, health or safety of any individual.
Correction of personal information	If an organisation holds personal information about an individual, and believes the information to be inaccurate, out of date, incomplete, irrelevant or misleading, it must take reasonable steps to correct the information. Similarly, it must do this if the individual requests.