

# UniSA Health Privacy Policy

UniSA Health Pty Ltd ACN 153 422 112 (**we, us, our**) is [bound by] the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth) (**Privacy Act**). We understand the importance of, and are committed to, protecting personal information. This Privacy Policy explains how we manage personal information (that is, information or an opinion, whether true or not, about an identified individual or an individual who is reasonably identifiable), including our obligations and the rights of individuals in respect of our dealings with personal information.

Please take a moment to read our Privacy Policy as it describes what happens to personal information, including sensitive personal information, that is collected via the UniSA Health Clinics (**Clinics**).

## 1. Policy

### 1.1 Collection

#### Personal Information

We will only collect and hold personal information if:

- (a) it is reasonably necessary for us to conduct our functions and activities;
- (b) it is able to do so in a lawful, transparent and non-intrusive way; or
- (c) it is required to do so by law.

We may collect personal information from individuals generally through some of the following means:

- (d) when an individual contacts a Clinic via telephone or facsimile;
- (e) when an individual completes a form for the purpose of registering with a Clinic;
- (f) from correspondence (whether in writing or electronically);
- (g) through any websites or mobile applications utilised by the Clinics to facilitate the provision of a health service;
- (h) while conducting customer satisfaction and market research surveys;
- (i) when administering any of our health services; and
- (j) as otherwise required to manage our business.

Where it is reasonably practical to do so, we will collect personal information directly from the relevant individual.

When it is not practicable or reasonable to obtain personal information from the individual to whom the information relates, personal information may be obtained from someone other than the individual to whom the information relates. If this occurs, we will take reasonable steps to ensure that the individual is made aware that the personal information was obtained from a third-party, and why this was necessary and reasonable in the circumstances.

We may also collect personal information:

- (a) provided on an individual's behalf with that individual's consent;
- (b) from a health service provider who refers the individual to a health practitioner providing a health services at or from the Clinics; or
- (c) from a health service provider to whom an individual is referred.

#### Sensitive personal information

Generally, we will only collect sensitive personal information, most particularly an individual's health information, where the individual has given their consent to that collection, unless otherwise permitted by law.

Situations where we may be permitted under law to collect an individual's health information without their consent include where the health information is necessary:

- (d) to provide a health service to the individual;
- (e) for research relevant to public health or public safety;
- (f) for the compilation or analysis of statistics relevant to public health or public safety; or
- (g) for the management, funding or monitoring of a health service.

## **2. Types of personal information we collect**

We may collect a range of personal information about an individual, including, but not limited to:

- (a) their name, gender and date of birth;
- (b) residential postal address and telephone number;
- (c) email;
- (d) bank account and financial details;
- (e) government related identifiers; and
- (f) their employment information.

We may also collect sensitive personal information, most particularly "health information".

Health information we may collect includes, but is not limited to, the following:

- (a) information about an individual's physical or mental health, both current and historical;
- (b) family medical history (where clinically relevant);
- (c) 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;
- (d) notes of an individual's symptoms or diagnosis and the treatment given;
- (e) specialist reports and test results;
- (f) appointment and billing details;
- (g) prescriptions and other pharmaceutical purchases;
- (h) dental records;
- (i) records held by a fitness club about an individual;
- (j) information about an individual's suitability for a job, if it reveals information about the individual's health;
- (k) an individual's healthcare identifier when it is collected to provide a health service; or
- (l) any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service.

Where an individual does not wish to provide us with their personal information, including sensitive personal information, we may not be able to provide the requested health service. In particular, a health practitioner may be unable to communicate with other health practitioners regarding the healthcare of an individual if the individual is unwilling for us to collect their personal information.

### **3. Use and disclosure of personal information**

#### Use of personal information

Personal information, including health information, collected by us may be used:

- (a) for the purpose advised to the individual at the time of collection of the information;
- (b) to provide health services and any ongoing related services to the individual, including education services;

- (c) to contact the individual, including for the purpose of:
  - (i) discussing their well being and progress after their initial appointment at a Clinic; and
  - (ii) gauging their interest in participating in research studies or clinical trials related to their health care.
- (d) as required for the ordinary operation of our services, including for the purpose of:
  - (i) obtaining cross-referral recommendations; and
  - (ii) referring the individual to a medical specialist or other health practitioner; and
- (e) for administrative, billing and insurance purposes;
- (f) for the purpose of liaising with government offices regarding Medicare entitlements and payments;
- (g) for the purpose of health and medical research;
- (h) where there is a serious and imminent threat to an individual's life, health, or safety, or a serious threat to public health or public safety; or
- (i) as required under compulsion of law, including for the purpose of satisfying mandatory notification obligations under the Health Practitioner Regulation National Law

We will not use or disclose personal information for any other purpose unless permitted under the APPs, or where the individual has consented to that use or disclosure.

#### Disclosure of personal information

We will take reasonable steps to ensure that an individual's personal information, including their health information, is not disclosed to a third-party, except in certain permitted situations. These include where disclosure is made:

- (a) with the consent of the individual;
- (b) for the purpose of referring the individual to another health practitioner;
- (c) to research institutions with whom we collaborate;
- (d) to private health insurance providers and Medicare Australia;
- (e) to anyone expressly authorised by the individual to receive their personal information; or
- (f) to any third party that we are required by law to disclose the individual's personal information to.

If we disclose personal information to a third party, we generally require that the third party protect personal information to the same extent that we do.

#### **4. Anonymised and de-identified information**

Where information is de-identified, aggregated or otherwise anonymised, such that an individual is not reasonably identifiable from this information, it will not constitute personal information and is not subject to the APPs. We may use and disclose such anonymised information for any purposes as we see fit, including to third parties for research and educational purposes.

#### **5. Protection of personal information**

We will take reasonable steps to protect personal information we hold from:

- (a) misuse, interference and loss; and
- (b) unauthorised access, modification or disclosure.

We have in place:

- (c) computer software and hardware that provides electronic protection of and/or prevents access to personal information from unauthorised persons, particularly from those individuals who are external to us. Electronic protection will include:
  - (i) mandatory password protection on computers; and
  - (ii) firewall and anti-virus software;
- (d) documented record management procedures in relation to the collection, physical security and storage of hard copy records; and
- (e) systems to manage all personal information so that it is able to destroy or permanently de-identify personal information, wherever reasonable and practicable, that is no longer needed for any reason.

#### **6. Data Breaches**

We have a Data Breach Response Plan in place and will manage all data breaches in accordance with the Notifiable Data Breaches (**NDB**) Scheme in Australia.

In accordance with the NDB Scheme, in the event of a suspected data breach we will:

- (a) contain the breach and, if possible, take remedial action; and
- (b) commence the requisite assessment process to determine whether the data breach is likely to be an "eligible data breach" for the purposes of the NDB Scheme. An "eligible data breach" being one where:
  - (i) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by us;

- (ii) the access, disclosure or loss is likely to result in "serious harm" to any of the individuals to whom the information relates. In this context, "serious harm" refers to serious physical, psychological, emotional, financial or reputational harm to an individual or individuals; and
- (iii) we have not been able to prevent the likely risk of serious harm with remedial action.

If we have reasonable grounds to believe that an "eligible data breach" has occurred, we will:

- (c) prepare a statement to the Office of the Australian Information Commissioner (**OAIC**) as soon as practicable (**OAIC Statement**);
- (d) notify the individual to whom the information relates as soon as practicable after the statement has been prepared; and
- (e) provide that individual with a copy of the OAIC Statement.

If we are unable to locate the individual to whom the eligible data breach relates for the purpose of providing them with a copy of the OAIC Statement, a copy of the OAIC Statement will be posted on the University of South Australia's website

## 6. Direct marketing

We will, on occasion, and where reasonable and appropriate, use an individual's personal information for the purpose of direct marketing. This includes providing them with information about new products, services and promotions offered by either us, or a third party, which are related to the health care of the individual and may be of interest to them.

Direct marketing in these circumstances may occur by mail, email, SMS or telephone.

Where the direct marketing is transmitted electronically or by telephone, we will at all times comply with any applicable laws including the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth).

We will not disclose personal information, including sensitive personal information, to third parties for a direct marketing purpose unless permitted by the APPs, or where we have been given consent to do so by the individual involved.

An individual may opt out at any time if they no longer wish to receive commercial messages from us. This request can be made by contacting us via the opt- out mechanism in the direct marketing material, or by contacting the Privacy Officer.

## 7. Consent

By providing sensitive information about yourself (or your spouse, partner or child) to us for the purpose of utilising the services provided by the Clinics, you will be considered to have given:

- (a) your consent to the collection and use of your sensitive information in accordance with this Privacy Policy;
- (b) in respect of sensitive information you provide to us on behalf of any person under 18 years of age, their consent to the collection of that sensitive information about them from you, and to the use of their sensitive information in accordance with this Privacy Policy; or
- (c) in respect of sensitive information you provide to us on behalf of any person over 18 years of age, their consent to the collection of that sensitive information about them from you, and to the use of their sensitive information in accordance with this Privacy Policy, with their authority.

## **8. Accessing and correcting personal information**

We will deal with requests for access or correction, by an individual, of their personal information held by us, in accordance with this policy.

Requests must be made in writing, and in the appropriate form specified by us from time to time.

On receipt of an application, and within a reasonable timeframe, we will take reasonable steps to inform the individual who made the request:

- (a) what personal information we hold in relation to that individual;
- (b) why the personal information is held;
- (c) how we collect (or collected), hold (or held), use (or used) and disclose (or disclosed) the personal information.

We will confirm with the individual whether they wish to have access to the personal information in question.

We will ordinarily give an individual access to their personal information unless an exception applies. Exceptions include where:

- (d) giving access would have an unreasonable impact on the privacy of other individuals;
- (e) the request for access is frivolous or vexatious; or
- (f) the access would be unlawful.

We reserve the right to charge a reasonable fee for providing access to the personal information, but no fee will be charged for making the application or correcting personal information held by us. We may withhold access to the personal information until the fee is paid.

If a request for access or correction is denied by us we will, within a reasonable time period, provide the individual who made the request with a general, written explanation as to why the request was refused. We will also take such steps, if any, as are

reasonable in the circumstances to give access in a way that meets our needs, and the needs of the individual.

## **9. Overseas transfers of personal information**

As at the date of this Privacy Policy, we are not likely to disclose personal information to overseas recipients, unless a health practitioner directs us to send an individual's personal information to a particular overseas recipient. The countries in which the overseas recipients will be located will be the countries nominated in accordance with the request.

If in future we do propose to disclose personal information overseas, we will do so in compliance with the requirements of the Privacy Act. We will, where practicable, advise of the countries in which any overseas recipients are likely to be located.

From time to time we may engage an overseas recipient to provide services to us, such as cloud-based storage solutions. Please note that the use of overseas service providers to store personal information will not always involve a disclosure of personal information to that overseas provider.

Each individual providing personal information to us consents to us disclosing this personal information to any such overseas recipients for purposes necessary or useful in the course of operating our business, and agrees that APP 8.1 will not apply to such disclosures. For the avoidance of doubt, in the event that an overseas recipient breaches the Australian Privacy Principles, that entity will not be bound by, and the individual will not be able seek redress under, the Privacy Act.

## **10. Accuracy**

We will be obliged, without an individual's request for correction, to correct inaccurate, out-of-date, incomplete, irrelevant or misleading personal information if we are satisfied that, having regard to the purpose for which the personal information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

If this occurs, we will take all reasonable steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

If an individual is of the view that their personal information requires correction, they should contact the Privacy Officer listed below.

## **11. Resolving personal information concerns**

If there any questions, concerns or complaints about this Privacy Policy, or how we handle personal information, please contact our Privacy Officer:

### **The Privacy Officer**

Privacy Officer  
GPO Box 2471  
Adelaide SA, 5001



Email: [privacy.officer@unisa.edu.au](mailto:privacy.officer@unisa.edu.au)

We take all complaints seriously, and will respond to each complaint within a reasonable period.

If dissatisfied with the handling of a complaint, an individual may contact the Office of the Australian Information Commissioner:

**Office of the Australian Information Commissioner**

GPO Box 5218

Sydney NSW 2001

Telephone: 1300 363 992

Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

## **12. Changes**

We reserve the right to change the terms of this Privacy Policy from time to time, without notice. An up-to-date copy of our Privacy Policy is available on the University of South Australia's website located at [www.unisa.edu.au/Campus-Facilities/community-clinics/](http://www.unisa.edu.au/Campus-Facilities/community-clinics/)

The last update to this document was 24/05/2018.