

HR+ Privacy Policy

Primary Health Workforce Team

Purpose

HR+ is committed to protecting and upholding the right to privacy of clients, staff, participants, external stakeholders, and website visitors. HR+ adheres to the Australian Privacy Principles (APP's) and complies with the Privacy Act 1988 (Cth). This policy details the way in which personal information is collected, used, stored, disclosed and destroyed by the Primary Health Workforce Team within HR+ in accordance with these privacy principles.

Scope

This policy applies to all HR+ staff, clients and stakeholders associated with the Primary Health Workforce (PHW) Team. It relates to the collection, storage, use, disclosure and disposal of all personal information handled by the HR+ PHW Team.

Definitions

Personal Information refers to information that is specific to an individual and could identify that individual.

Sensitive Information is a specific type of personal information that is sensitive in its nature and attracts a higher level of privacy protection than other personal information. Sensitive information can include:

- ▶ racial or ethnic origin
- ▶ political opinions or associations
- ▶ religious or philosophical beliefs
- ▶ trade union membership or associations
- ▶ sexual orientation or practices
- ▶ criminal record
- ▶ health or genetic information
- ▶ some aspects of biometric information

Policy Statement

To carry out day-to-day business functions HR+ is required to collect a variety of personal information from clients, staff and sometimes other stakeholders. Any information collected has direct relevance to HR+ business purposes and to the fulfilment of a function of these business purposes. HR+ is obliged to comply with the relevant legislation regarding the handling of information and in doing so HR+ ensures that each individual

- ▶ Knows why their information is being collected, how it will be used and who it will be disclosed to.
- ▶ Consents to the collection of any sensitive information.
- ▶ Is provided with access to the current privacy policy.
- ▶ Can access their personal information upon request.
- ▶ Can ask for personal information that is incorrect to be corrected.

- › Does not receive unwanted direct marketing.
- › Can make a complaint if they feel their information has been mishandled.

Procedures

Collection of Personal Information

In general, personal information will be collected directly using standard registration forms, applications, contracts, HR+'s website, and via emails and phone conversations. Whenever HR+ collects information, the purpose of collection will be explained as well as how the information will be used and who it might be provided to. If unsolicited information is received, HR+ will either provide a **Consent to the Collection and Use of Information Form** in order to use and store the information or destroy the information, if it is not information that HR+ require for the purpose it has been provided.

Consent must be obtained when collecting personal information that is deemed sensitive. Consent is collected using HR+'s **Consent to the Collection and Use of Information Form**. Consent must be informed whereby the individual in question understands the consequences of giving or not giving consent and HR+ staff have clearly explained how they will handle the relevant information.

Consent is voluntary and should include the option not to consent, including an explanation of potential outcomes should a person refuse to consent.

Consent must be current and specific. Consent cannot be assumed to continue indefinitely. HR+ staff will ensure that when asking for consent, they explain the reason for their request (as specific as possible) and that a timeframe is provided suitable to the collection and usage of the relevant information.

At times, personal information may be collected from a third party, or publicly available source, but only if the individual has consented to such collection or would reasonably expect HR+ to collect their information in this way. A third party might include regulatory bodies or colleges.

The types of personal information collected might include:

- › Full name
- › Passport and visa information
- › Photographic identification
- › Contact details e.g., phone, email, residential and postal address, emergency and/or primary contacts
- › Demographic information e.g., age, date of birth, gender, occupation
- › Sensitive information e.g., racial or ethnic origin, disability, religion
- › Bank details in the case of scholarships and event registration
- › Education information
- › Practice information
- › Any additional information relating to the individual that is provided to us directly through our website or referral pathways

Use and Disclosure of Personal Information

HR+ will only use and disclose personal information for the primary purposes for which it was collected, which might include administering recruitment and placement services, providing scholarships, practice management support, processing requests to participate in conferences and events and facilitating ongoing support through to independent practice.

Exceptions include when

- ▶ The individual has consented to the information being used for a secondary purpose.
- ▶ The individual would reasonably expect HR+ to use or disclose the information for a secondary purpose and that purpose is related to the primary purpose.
- ▶ The use or disclosure of the information is required or authorised by or under an Australian law or court/tribunal order.
- ▶ HR+ reasonably believes the use or disclosure of the information is necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

HR+ will only use sensitive information for a secondary purpose if it is directly related to the primary purpose.

Client personal information might be shared with regulatory and funding bodies including AHPRA and Government Departments, as well as colleges.

Storage of information

HR+ is committed to taking all reasonable steps to ensure that the information provided to us is secure. Information is held electronically on HR+'s cloud-based Client Relationship Manager (CRM). Access to information is limited to the personnel with the correct authorisation and only as many staff members as necessary are provided with access to client information. All HR+ staff members sign a non-disclosure agreement upon employment. All paper-based records are held only long enough to electronically store and then they are shredded. Where staff leave the organisation their access to data is removed. HR+ takes all reasonable measures to protect personal information from unauthorised access, improper use, disclosure, unlawful destruction and accidental loss. Should a breach occur, staff follow the steps outlined in the **Data Breach Response Plan** using the **Data Breach Incident Report Form**.

Access to information

HR+ acknowledges the rights of individuals to have access to their personal information and to request amendments to this information. Clients are encouraged to update their information as it changes to maintain the currency and accuracy of HR+ records. An individual may request details of personal information that we hold about them in accordance with the Privacy Act 1988 (Cth). If they would like a copy of the information or believe that any information we hold is inaccurate, out of date, incomplete, irrelevant, or misleading, this should be addressed in writing to HR+. For a person to request a copy, or a correction, of their personal information they must contact the Primary Health Workforce Team Manager in writing and provide identification.

HR+ reserve the right to refuse to provide an individual with their information in certain circumstances set out in the Privacy Act.

HR+ can refuse to give a person access to their personal information if:

- ▶ It may threaten their own or someone else's life, health, or safety
- ▶ It may impact someone else's privacy
- ▶ Giving access would be unlawful

If giving the person certain information would impact someone else's privacy, HR+ may de-identify areas of the information and provide the remainder. If it's not possible to give information directly to someone because of a concern for their health and safety, then we may give access through an agreed third-party.

Destruction of information

HR+ will only retain information for as long as the information is required to fulfil the purpose it was collected for. This generally includes administering recruitment and placement services, providing scholarships, providing practice management support and facilitating ongoing support through to independent practice. Where an individual is no longer being provided with this service from HR+, any personal information will be destroyed or deidentified within twelve months with the assistance of the relevant Information Technology providers used.

Complaints

If an individual has a complaint about the way in which their information has been collected, stored, disclosed or used by HR+, please refer to HR+'s **Complaints Policy** for complaints procedure.

Forms and Relevant Documents

1. Consent to Collection and Use of Information Form
2. Record Management Policy
3. Complaints Policy and Procedure
4. Data Breach Response Plan
5. Data Breach Incident Report Form

Authorised by the CEO		
Signature		Date Adopted: 5 May 2022 Date Reviewed: 22 August 2023
Name	Peter Barns	Review Due: August 2024