# Privacy Policy

## 1. Introduction

The purpose of this policy is to advise external parties that we (iRecruit Medical (iRM) Pty Ltd ABN 37628200297) are committed in managing personal information in accordance with the Privacy Act 1988 and any of its amendments, Privacy Amendment (Enhancing Privacy Protection) Act 2012 which outlines the Australian Privacy Principles

We only collect information that is reasonably necessary for the proper performance of our activities or functions.

We do not collect personal information just because we think it could be useful at some future stage if we have no present need for it.

We may decline to collect unsolicited personal information from or about you and take steps to remove it from our systems.

By following the links in this document, you will be able to find out how we manage your personal information as an APP Entity under the Australian Privacy Principles (APPs).

You will also be able to find out about the information flows associated with that information.

## 2. Information Flow

When we collect your personal information:

- we check that it is reasonably necessary for our functions or activities as a Medical Recruitment agency, placement and services firm.
- we check that it is current, complete and accurate. This will sometimes mean that we must cross check the information that we collect from you with third parties;
- we record and hold your information in our Information Record System. Some information may be disclosed to overseas recipients
- we retrieve your information when we need to use or disclose it for our functions and activities. At that time, we check that it is current, complete, accurate and relevant. This will sometimes mean that we must cross check the information that we collect from you with third parties once again - especially if some time has passed since we last checked.

- we destroy or de-identify your personal information when it is no longer needed for any purpose for which it may be used or disclosed if it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record.

## 3. Kinds of information that we collect and hold

Personal information that we collect and hold is information that is reasonably necessary for the proper performance of our functions and activities as a Medical Recruitment agency, placement and services firm and is likely to differ depending on whether you are:

- a Workseeker
- a Client
- a Referee

## 4. Purposes

The purposes for which we collect, hold, use and disclose your personal information are likely to differ depending on whether you are:

- a Workseeker
- a Client
- a Referee

The following sections are also relevant to our use and disclosure of your personal information including Marketing and Overseas disclosures

### For Workseekers

Information that we collect, hold, use and disclose about Workseekers is typically used for:

- work placement operations;
- recruitment functions;
- statistical purposes and statutory compliance requirements;

### For Clients

Personal information that we collect, hold, use and disclose about Clients is typically used for:

- client and business relationship management;
- recruitment functions;
- marketing services to you;
- statistical purposes and statutory compliance requirements;

### For Referees

Personal information that we collect, hold, use and disclose about Referees is typically used for:

- to confirm identity and authority to provide references;
- Workseeker suitability assessment;
- recruitment functions;

## 5. Direct Marketing

We may contact you in relation to new products and services and undertake direct marketing activities from time to time. If you do not want to participate in any of those activities or do not want to receive direct marketing from us, you can tell us that you wish to opt out of these direct marketing activities by contacting us on enquiry@irecruitmedical.com.au.

## 6. How your personal information is collected

We collect information about you and the interactions you have with us. This includes when you request or use our services, seek employment with or through us, and when you communicate with us on the phone, email, through our websites, apps and mobile applications.

Depending on the nature of the services we provide and type of relationship we have with you, we may Collect information about your identity and contact details, your gender, your nationality and right to work in Australia, information relating to equal opportunity, your health and fitness, employment history, qualifications and related information.

If you use our website, apps, online services and other mobile applications, information about your location and activities may also be collected. Such information includes IP addresses, telephone numbers and whether you accessed third party sites. It also includes information on the volume of sites, date and time of visits, the origin of visits, pages viewed and length of time spend on our site. (Some of this information is collected through the use of our cookies (see information below on cookies)

We may request that you supply photographs and scan photo ID. Please do not Upload photographs of any individuals who have not given consent to the display of their photograph. Displaying photographs without that person's consent may breach privacy laws.

## 7. How we use cookies

We will use combination of the various types of cookies from time to time. Our use of cookies will depend on what part of our website and online services you use and what functions you request of the site and service,

We use cookies for the following purposes:

- To help us analyse the use and performance of our website and services.
- To help display advertisement.
- To help us determine if you are logged into our website.
- To store information about your preferences and to personalise the website for you.
- For security purposes.
- To identify you when you visit our website and as you navigate.

## 8. How we keep your information secure

We generally keep our records that contain your information on our premises and systems but some offsite using trusted third parties.

We have a secure database for storing your information. We also train and remind our staff to their obligations with regard to your information.

We interact with you on the internet through our website, apps, online services and mobile applications, we generally use a variety of tools and systems to protect against unauthorised persons and viruses accessing our systems.

We generally only keep information for as long as required. For example, to be able to provide ongoing services and opportunities and to meet legal obligations and internal needs.

Reasonable steps are taken to ensure your personal information is protected from misuse, loss, unauthorised access, modification or disclosure. In the even that any personal information has been lost or subjected to unauthorised access, use, modification, disclosure or other misuse (Data Breach), iRM will take all the necessary steps to immediately contain and rectify the Data Breach and prevent the Data Breach from future reoccurrence.

## 9. Notifiable Data Breach

An Eligible data breach occurs when the following criteria are present:

- There is unauthorised access to, or unauthorised disclosure of personal information that we hold; and
- This is likely to result in serious harm to one or more individuals; and
- We have not been able to prevent the likely risk of serious harm with remedial actions (Serious harm may be psychological, emotional, physical or reputational).

If an Eligible data breach is found, we would complete the following steps which are further outlined in our Company Notifiable Data Breach Plan:

- Conduct an assessment immediately to investigate the matter. The 3 steps involve;

    1. Initiate the assessment.
    2. Investigate and gather information.

3. Evaluate and make a decision whether it has indeed been an eligible data breach (there is a maximum of 30 days to conduct assessments);

- We would ensure the relevant personnel were made aware of the breach as practicable
- We would notify the breach as soon as practicable once we believe and eligible data breach has occurred. To individuals whose personal information is involved, Publish and publicise the notification where required.

## 9. Disclosures

We may disclose your personal information for any of the purposes for which it is primarily held or for a lawful related purpose.

We may disclose your personal information where we are under a legal duty to do so. Disclosure will usually be:

- internally and to our related entities
- to our Clients
- to Referees for suitability and screening purposes.
- Background checking and screening agents;
- Travel and booking agents
- Software solutions providers;

### Cross-Border Disclosures

Some of your personal information is likely to be disclosed to overseas recipients. We cannot guarantee that any recipient of your personal information will protect it to the standard to which it ought to be protected.

When we send your information overseas, we will make sure that the appropriate security arrangements and data handing systems are in place. Please note that in some cases, overseas laws may apply to the data.

## 10. Access & Correction

Subject to some exceptions set out in privacy law, you can gain access to your personal information that we hold.

Important exceptions include:

- evaluative opinion material obtained confidentially in the course of our performing reference checks; and access that would impact on the privacy rights of other people. In many cases evaluative material contained in references that we obtain will be collected under obligations of confidentiality that the person who gave us that information is entitled to expect will be observed. We do refuse access if it would breach confidentiality. If there are extenuating circumstances, we can obtain consent from the referees and provide you with information upon their approval

### Access Policy

If you wish to obtain access to your personal information you should contact our Privacy Co-ordinator. You will need to be able to verify your identity.

Access to your information needs to be in writing and to allow us 14 days to respond as per legislative requirements. We will endeavour to respond earlier than this time and usually there should be no problems in sharing access to your data.

- Any lawful costs or charges that you impose on iRM to obtain any information will be passed on to you if required;
- We will respond to your request within 14 days of receipt of request and will keep you updated as to the process of obtaining the required information as the matter proceeds;
- Generally, requests for information access will be accepted, however in the event that we do not have to provide the information we may refuse the request and you will be informed in writing as to the reason for the refusal including an explanation as to why;
- Any complaints will be directed to our Senior Management to respond to in a fair and reasonable manner, we will always take complaints seriously.

### Correction Policy

If you believe we hold inaccurate information about you or have provide to others, you can ask us to correct the information by contacting us in writing.

## 11. Making a privacy complaint

If you have a concern about your privacy, you have the right to make a complaint. If you make a complaint we will do everything we can to put matters right. It should be first made to us in writing,

You can make complaints about our handling of your personal information to our Privacy Co-ordinator on enquiry@irecruitmedical.com.au or phone 03 93978458