Medic Oncall™
By Healthcare Australia

V3 February 2021

# Medic Oncall by Healthcare Australia Privacy Policy

## 1. Introduction

We manage your personal and health information in accordance with the Privacy Act 1988 and the Australian Privacy Principles. This policy applies to information collected by Healthcare Australia Pty Ltd trading as Medic Oncall by Healthcare Australia (the Company).

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 may take steps to purge it from our systems.

In this document, you will be able to find out how we manage your personal information as an APP Entity under the APP's.

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

### 1.1 APP Entity

The Company manages personal information, as an APP Entity, under the Australian Privacy Principles.

Because we are a contracted service provider to a range of Commonwealth, State and Territory government agencies, it sometimes becomes necessary for us to collect and manage personal information as an Agency under different privacy arrangements. If you wish to know whether this applies to you, please contact us.

### 1.2 Information Flow

When we collect your personal information:

- we use our best endeavours to check that it is reasonably necessary for our functions and activities as a recruitment and workforce management company including the purposes of sourcing, recruitment and placement of candidates to suit clients requirements;
- we check that it is current, complete and accurate. This will sometimes mean that we have to cross check the information that we collect from you with third parties;
- we record and hold your information in our secure Information Record System and in the Cloud;
- we retrieve your information when we need to use or disclose it for our functions and activities including sourcing, recruitment and placement of candidates to suit clients requirements and we check that it is current, complete, accurate and relevant and may update this information each twelve months. This will sometimes mean that we have to cross check the information that we collect from you with third parties once again - especially if some time has passed since we last checked;
- subject to some exceptions, (7. Access & Correction) we permit you to access your personal information in accordance with APP:12 of the APP's);
- we correct or attach associated statements to your personal information in accordance with APP:13 of the APP's;
- 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 provided that it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record.

## 2. 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 recruitment and workforce management company and is likely to differ depending on whether you are:

- a medical practitioner;
- a Client;
- a Referee.

### 2.1 For Medical Practitioners

The type of information that we typically collect and hold about Medical Practitioners is information that is necessary to assess amenability to a placement or assignment and work offers availability; to meet credentialing and other registration requirements of our Clients; to meet any legal or legislative requirement; suitability for placements and/or assignments; or to manage the performance in work obtained through us and includes:

- Resume;
- References;
- Medical Registration;
- Medical Indemnity;
- Australian Business Number;
- Medical Prescriber number;
- Citizenship/working rights in Australia;
- 100 points Identity Check;
- Working with children Check;
- Your photograph so we can produce your Photo Identification Card for you to use and wear when working at client premises;
- As an accredited body with the Australian Criminal Intelligence Commission (ACIC) for the purpose of conducting National Criminal History Checks, we may collect information for this purpose including your informed consent and additional identity documents if required to conduct the National Criminal History Check;
- Other relevant information to secure short term and long term work placement and/or assignment with clients;
- History of placements including dates;
- Customer feedback on work performance and placement capability;
- If you consent, we may also collect sensitive information (for example, health information). It is up to you to choose the information that you give to us. If you choose not to provide us with particular information that has been requested, we may not be best placed to provide the service that you have requested and may impact our ability to find suitable assignments and placements.

### 2.2 For Clients

The type of information that we typically collect and hold about Clients is information that is necessary to help us manage the presentation and delivery of our services and includes:

- Name, address, contact person, other relevant information about the facility including size and structure, medical departments, heads of department;
- Feedback about our services and the performance of medical practitioners placed and/or assigned to clients;
- Placement, assignment and usage history with us.

### 2.3 For Referees

The type of information that we typically collect and hold about Referees is information that is necessary to help to make determinations about the suitability of one of our Medical Practitioners for particular jobs or particular types of work and includes:

- Name, location and professional working relationship to the Medical Practitioner.

## 3. Purposes

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

- a Medical Practitioner;
- a Client;
- a Referee.

The following sections are also relevant to our use and disclosure of your personal information:

- Our Policy on Direct Marketing;
- Overseas Disclosures.

### 3.1 For Medical Practitioners

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

- short and/or long term work placement and/or assignment operations;
- short term and/or long term recruitment functions;
- statistical purposes and statutory compliance requirements.

### 3.2 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.

### 3.3 For Referees

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

- confirming identity and authority to provide references;
- Medical Practitioner suitability assessment;
- recruitment functions.

### 3.4 Our Policy on Direct Marketing

- Personal information might be used for marketing purposes directly or by a third party if that third party is a co-sponsor of a Company event;
- Customer lists are not given to third parties for marketing purposes;
- Individuals have the option as to whether or not they wish to receive our e-newsletter and can unsubscribe at any time they wish;
- The Company is compliant with the requirements of the anti-spam legislation.

## 4. How your personal information is collected

The means by which we will generally collect your personal information are likely to differ depending on whether you are:

- a Medical Practitioner;
- a Client;
- a Referee.

We sometimes collect information from third parties and publicly available sources when it is necessary for a specific purpose such as checking information that you have given us or where you have consented or would reasonably expect us to collect your personal information in this way.

Sometimes the technology that is used to support communications between us will provide personal information to us see the section in this policy on Electronic Transactions (4.5 Electronic Transactions). See also the section on Photos & Images (4.4 Photos & Images)

### 4.1 For Medical Practitioners

Personal information will be collected from you directly as part of your application and membership with us and will include information required as part of our checking and credentialing process, required as part of our Client's checking and credentialing process, and in connection with you seeking placement and/or assignment work through us.

- We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet, social media sites and a number of third parties. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

### 4.2 For Clients

Personal information about you may be collected:

- when you provide it to us for business or business related social purposes;
- to assist in meeting your locum and staffing requirements.
- We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

### 4.3 For Referees

Personal information about you may be collected when you provide it to us:

- in the course of our checking references processes and procedures;
- when we are checking information that we obtain from you about Medical Practitioners.
- We may also collect personal information about you from a range of publicly available sources including newspapers, journals, directories, the Internet and social media sites. When we collect personal information about you from publicly available sources for inclusion in our records we will manage the information in accordance with the APPs and our Privacy Policy.

### 4.4 Photos & Images

As part of the Company's registration and credentialing processes, we will ask you to provide photo identification to assist with our checking procedures. We will also request a photo from you (if you haven't supplied one with your resume) to enable us to produce your Company Identification Card which you are required to wear when you work with our clients. We will retain a copy of your Identification Card however this Identification Card is not used for any other purpose.

From time to time our clients request copies of your identification and check documents to confirm your identity and when we send these they may contain photo identification that you have provided to us. If you do not wish us to take a copy or you do not wish us to send these checks to our clients, please advise us and we will discuss alternative Identification arrangements when you work with our clients.

### 4.5 Electronic Transactions

We collect personal information that individuals choose to give us via online forms, MOCApp or by email, for example when individuals:

- ask to be on an email list or other job notification list or MOCApp;
- register as a site user to access facilities on our site such as a job notification board or other information;
- use the MOCApp to register, access available work and other uses available on the MOCApp;
- make a written online enquiry, enquire using the MOCApp or email us through our website;
- submit a resume by email, MOC App or through our website;
- submit other documentation required to register with us and to work with our clients and customers.

It is important that you understand that there are risks associated with use of the Internet and you should take all appropriate steps to protect your personal information. It might help you to look at the OAIC's resource on Internet Communications and other Technologies.

When you visit our websites, we may collect information you have given us when: (a) registering or subscribing to our services or requesting further services on any of our websites or Apps; (b) contact us to report a problem with our websites or Apps or make any enquiry or query or comment; and (c) you apply online on our website or MOCApp for a job or work with us, you may need to provide (without limitation) information about your education, identification checks, employment history, medical credentials and other documents required by our Clients. Your application will constitute your express consent to us to use this information to access your application and to allow us to carry out any services and other related activities as may be required of us under applicable law.

We collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the website. We will not associate any data gathered from this site with any personally identifying information.

You can contact us by telephone or post if you have concerns about making contact via the Internet.

The Company takes reasonable steps to keep personal information secure, accurate and up to date. The Internet is not always a secure method of transmitting information. Accordingly, while we seek to protect your personal information by implementing digital security systems in various parts of our website or App, The Company cannot accept responsibility for the security of information you send to or receive from us over the Internet or for any unauthorised access or use of that information. Where we have links to websites outside the Company we cannot ensure that your privacy will be protected in accordance with this policy. You should consult these other websites' privacy policies as we have no control over them and are not responsible for any information that is submitted to or collected by these third parties.

The Company is committed to complying with Australian Privacy Principles and operates its information management systems and database with high commitment to security and maintains regular and ongoing security arrangements across Computing Services including Cloud, Mail, Call and Message Logs, Social Media and Mobile Access.

## 5. How your personal information is held

Personal information is held in our Information Record System and in the Cloud until it is no longer needed for any purpose for which it may be used or disclosed at which time it will be de-identified or destroyed provided that it is lawful for us to do so.

We take a range of measures to protect your personal information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

### 5.1 Our Information Record System and Cloud

Our information management system comprises electronic format and hardcopy format of information. Hardcopy information is only available to specific staff that may be required to access this information to perform our functions and activities. All hardcopy formats are securely stored in locked storage cabinets. Electronic information is stored on our secure database and/or the Cloud and only retrieved when necessary to perform our functions and activities.

Where we use the Cloud, we will take reasonable steps to ensure that:

- Disclosure of your personal information to the cloud service provider is consistent with our disclosure obligations under the Australian Privacy Principals. This may include ensuring that we have obtained your consent, or that the disclosure is for purposes within your reasonable expectations;
- Disclosure is consistent with any other legal obligations;
- Our Cloud computing services provider's terms of service recognise that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations.

### 5.2 Information Security

Due to the nature of the personal and sensitive information we collect to perform our functions and activities we are committed to securing information by storing on our secure database and information records and in the Cloud. Regular checks are conducted to ensure our information security is not comprised.

We take a range of measures to protect your personal information from misuse, interference, loss unauthorised access, modification or disclosure and these measures include:

- Policies and procedures including need to know authorisation policies;
- Password protection;
- Policies on laptop, mobile phone and portable storage device security;
- Culling procedures including secure disposal and timely culling of information;
- Staff training;
- "Clean desk" procedures;
- Data breach response and notification procedures.

## 6. Disclosures

We may disclose your personal information for any of the purposes (3. 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 and service partners;
- to our Clients;
- to Referees for suitability and screening purposes.

### 6.1 Related Purpose Disclosures

We outsource a number of services to contracted service suppliers (CSPs) from time to time. Our CSPs may see some of your personal information. Typically our CSPs would include:

- Software solutions providers;
- I.T. contractors and database designers and Internet service suppliers;
- Legal and other professional advisors;
- Insurance brokers, loss assessors and underwriters;
- Service partners;
- Superannuation fund managers;
- Background checking and screening agents.

We take reasonable steps to ensure that terms of service with our CSPs recognise that we are bound by obligations to protect the privacy of your personal information and that they will not do anything that would cause us to breach those obligations.

### 6.2 Cross-Border Disclosures

Your information will not normally be shared across borders.

We do use the services of third party organisations from time to time that may use across border services, if this is the case 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. The costs and difficulties of enforcement of privacy rights in foreign jurisdictions and the impracticability of attempting to enforce such rights in some jurisdictions will mean that in some instances, we will seek your consent to disclosure.

## 7. 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.
- For more information about access to your information see (7.1 Access Policy).

For more information about applying to correct your information see (7.2 Correction Policy).

### 7.1 Access Policy

If you wish to obtain access to your personal information you should contact our Privacy Officer. You will need to be in a position to verify your identity. You will also be asked a number of questions and may be required to provide additional information. Usually we will require one week to respond to your request.

Where you request your personal information to be updated and there is a dispute about the facts, we will make a note on your personal information of such dispute. If you have created an account with The Company via our website or MOCApp, you are able to view and update some information by logging into your account.

You may also request that The Company stops using your information and contacting you and we will comply with your request (for example if at any time you would prefer to stop receiving newsletters and updates from us, please use the "unsubscribe" option included or respond to the email advising you would like to stop receiving information and other material). However, if this involves a request for deletion of your file, please be aware that we may not be required or able to do so, particularly where your file also holds information about our clients. We reserve the right to charge an administrative fee for access and updating requests.

### 7.2 Correction Policy

If you find that personal information that we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to correct it by contacting us.

We will take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose (3. Purposes) for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

If we have disclosed personal information about you that is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to notify the third parties to whom we made the disclosure and we will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so. We will respond promptly to correct any incorrect or out of date information.

We comply with Data Breach Response and Notification Procedures. For information on this response procedure please contact our Privacy Officer (Contact Us).

## 8. Complaints

You have a right to complain about our handling of your personal information if you believe that we have interfered with your privacy.

### 8.1 Complaints procedure

If you are making a complaint about our handling of your personal information, it should first be made to us in writing.

You can make complaints about our handling of your personal information to our Privacy Officer, whose contact details are (Contact Us).

We aim to acknowledge receipt as soon as possible and commit to resolve all complaints between 7 and 30 days. However, there may be instances where this is not possible due to the contents of the complaint. In such circumstances, we will respond to your complaint in a reasonable and practical time.

You can also make complaints to the Office of the Australian Information Commissioner.

Complaints may also be made to the RCSA, the industry association of which we are a member. RCSA administers a Code of Conduct for the professional and ethical conduct of its members. The RCSA Code is supported by rules for the resolution of disputes involving members.

NOTE: The Association Code and Dispute Resolution Rules do NOT constitute a recognised external dispute resolution scheme for the purposes of the APPs; but are primarily designed to regulate the good conduct of the Associations members.

When we receive your complaint:

- We will take steps to confirm the authenticity of the complaint and the contact details provided to us to ensure that we are responding to you or to a person whom you have authorised to receive information about your complaint;
- Upon confirmation we will write to you to acknowledge receipt and to confirm that we are handling your complaint in accordance with our policy;
- We may ask for clarification of certain aspects of the complaint and for further detail;
- We will consider the complaint and may make enquiries of people who can assist us to establish what has happened and why;
- We will require a reasonable time (usually within 1 week however in some cases up to 30 days) to respond;
- If the complaint can be resolved by procedures for access and correction (7. Access & Correction) we will suggest these to you as possible solutions;
- If we believe that your complaint may be capable of some other solution we will suggest that solution to you, on a confidential and without prejudice basis in our response.

  If the complaint cannot be resolved by means that we propose in our response, we will suggest that you take your complaint to any recognised external dispute resolution scheme to which we belong or to the Office of the Australian Information Commissioner.

## Contact Us

You can contact our Privacy Officer/Coordinator as follows:

**Email:** foirequest@healthcareaustralia.com.au

**Phone:** +61 2 9024 3241

Further information is available from the Office of the Australian Information Commissioner. (OAIC Privacy Information)