

1. INTRODUCTION

Cornerstone Medical Recruitment Pty Ltd manages personal information and is an *identified entity* in accordance with the **Privacy Act 1988**. This Policy addresses our compliance with the **Australian Privacy Principles (APPs)** and applies to information collected by Cornerstone Medical Recruitment Pty Ltd and all our operations in Australia.

As an *identified entity* we are also responsible for the protection of any personal information collected and comply to the best of our abilities with the **Identifiable Data Breaches Scheme**.

Cornerstone Medical Recruitment Pty Ltd is a national On Hire Employer and collects personal information such as Tax File Numbers (TFN's). As such we are a **Lawful Tax File Number Recipient**.

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 purge 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 APP.

1.1 PROTECTING YOUR PRIVACY

Cornerstone Medical Recruitment falls within the Australian Privacy Principles (APP) and manages personal information, in compliance with the Australian Privacy Principles as an APP Entity, under the Australian Privacy Principles APP. As 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.

This Privacy Policy and Collection Statement explains how we collect information, including your personal information, and how we maintain, use and disclose that information. It also provides some details about your privacy rights along with our general rights and obligations in relation to the information we keep on record.

1.2 INFORMATION FLOW

When we collect your personal information:

- We check that it is reasonably necessary for our functions or activities as a recruitment company and outplacement 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;
- 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;
- Subject to some exceptions, we permit you to access your personal information in accordance with AAP:12 APP;
- We correct or attach associated statements to your personal information in accordance with APP:13 APP;

- 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 it is lawful for us to do so. We do not destroy or de-identify information that is contained in a Commonwealth Record.

2. TYPES OF INFORMATION THAT WE COLLECT & 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 Service Provider, and is likely to differ depending on whether you are:

- A Job Seeker
- A Client
- A Referee

2.1 FOR JOB SEEKERS

The type of information that we typically collect and hold about Job Seekers is information that is necessary to assess the amenability to work offers and work availability; suitability for placements; or to manage the performance in work obtained through us and includes:

- Information about your past employment;
- Information about your employment aspirations;
- References;
- Confirmation of employment;
- Confirmation of past performance;
- Your eligibility to work in Australia;
- Your income expectations;
- Your geographical location and expectations;
- Information about your qualifications, skills and capabilities;
- Information about your professional registration;
- Information contained in documents that you provide during our recruitment process.

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:

- Information about your workplace relevant to recruitment projects;
- Information you provide to us in your job description;
- Information you provide to us in meetings, discussions and consultations;
- Information about your talent needs;
- Information about your recruitment and on-boarding processes;
- Information about the skills, experience, and talent you seek;
- Information contained in documents that you provide during our recruitment process.

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 Job Seekers for particular jobs, or particular types of work and includes:

- Your title and the organisation you work for;
- Information about how we can contact you in relation to conducting a reference check;
- Information about if you agreed or disagreed to act as a referee on the occasion when it was relevant to our recruitment process.

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 Job Seeker
- 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 JOB SEEKERS

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

- Work placement operations;
- Recruitment functions;
- Statistical purposes and statutory compliance requirements;
- Marketing services to you;
- Market research and reports.

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;
- Market research and reports.

3.3 FOR REFEREES

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

- Confirmation of identify and authority to provide references;
- Job Seeker suitability assessment;
- Recruitment functions;
- Confirmation of information provided to us by the Job Seeker.

4. OUR POLICY ON DIRECT MARKETING

We may utilise your information for direct marketing purposes. In addition:

- Your personal information will not be provided to third parties for direct marketing purposes;
- Customer lists are not obtained from third parties for marketing purposes;
- As a Job Seeker, your resume will be reformatted and de-identified before it is sent to a Client;
- We do provide you with the opportunity not to be included in our direct marketing activities;
- In line with Cornerstone Medical Recruitment's compliance with respect to anti-spam legislation, we have opt out functions on all of our direct marketing.

5. HOW YOUR PERSONAL INFORMATION IS COLLECTED

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

- A Job Seeker
- 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.

Please also see the section on Photos and Images.

5.1 FOR JOB SEEKERS

Personal information will be collected from you directly when you fill out and submit one of our application forms, apply on line, email your information directly to us, or provide us with any other information in connection with your application to us for work.

Personal information is also collected when:

- You provide us your information online or via email;
- During telephone discussions relevant to your work placement wants, needs and requirements;
- We undertake reference checking;
- We undertake confirmation of employment procedures;
- We undertake qualification and professional registration confirmation processes.

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 Australian Privacy Principles APP and our Privacy Policy.

5.2 FOR CLIENTS

Personal information about you may be collected when:

- You provide it to us for business or business related social purposes;
- You engage Cornerstone Medical Recruitment as a recruitment provider;

- You enquire about Cornerstone Medical Recruitment's recruitment service;
- Cornerstone Medical Recruitment prepares, submits or considers a tender or bid process with your organisation.

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 Australian Privacy Principles APP and our Privacy Policy.

5.3 FOR REFEREES

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

- While checking Job Seeker references with you;
- When we are checking information that we obtain from you about Job Seekers.

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 Australian Privacy Principles APP and our Privacy Policy.

6. PHOTOS & IMAGES

We will not request that you supply photographs, scan photo ID, or capture and retain video image data of you in cases where simply sighting photographs or proof of identify documents would be sufficient in the circumstances.

6.1 ELECTRONIC TRANSACTIONS & TELEPHONE TRANSACTIONS

Sometimes, we collect personal information that individuals choose to give us via online forms or by email, or during a telephone conversation, for example when individuals:

- Ask to be on an email list such as a job notification list;
- Register as a site user to access facilities on our site, such as a job notification board;
- Make a written online enquiry or email us through our website;
- Submit a resume by email or through our website;
- Communicate information to us about their job seeking requirements or recruitment requirements via email, telephone and voicemail;
- Send us an email which relevant attachments or content that is related to job seeking or recruitment processes.

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 QAIC's resource on Internet Communications and other Technologies. You can contact us by telephone or post, if you have concerns about making contact via the Internet.

6.2 GENERAL – VISITING OUR WEBSITE AND ONLINE

When you visit the Cornerstone Medical Recruitment website, we record anonymous information such as the date and time of your visit, the server/IP address, which site was visited, and the information viewed and/or downloaded. The information gathered cannot be directly matched to an individual and

is only used for administration and statistical purposes such as error logging. The information cannot tell us anything about you; it can only tell us about how you used our web site. This information can help us determine what areas of our website are most beneficial to our visitors. No attempt is made by Cornerstone Medical Recruitment to identify users or their browsing activities.

If you visit the Candidate Registration website and register on-line for employment opportunities or visit the client resources site to register a vacancy, we do collect some personal information about you which you volunteer by filling in your details. The information required may include providing basic personal details such as your name, address, phone number and email address etc. You may also submit your resume or a position description. The information gathered at this point is stored in our database for retrieval and use by Cornerstone Medical Recruitment staff only for the purposes for which it was intended. By submitting your personal information in this way, you acknowledge and accept our Privacy Policy and Collection Statement.

When submitting a time sheet via our website, the information is transmitted directly to our payroll division, where it is only used for the intended purpose and is not disclosed to anyone outside the organisation. There is no collection of personal information until you have completed the time sheet and submit to Cornerstone Medical Recruitment for processing.

We do not disclose any information gathered about your visit to our website, or personal information that you provide through the Candidate Registration process, such as your name, address etc. to any other organisation outside Cornerstone Medical Recruitment unless you give your express consent, or if we are required to do so by law.

At times you may forward an email to us via the email link in our website. The information collected through this email will only be used for the purpose for which you have provided it.

7. HOW YOUR PERSONAL INFORMATION IS HELD

Personal information is held in our Information Record System 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;
- Unauthorised access, modification or disclosure.

7.1 OUR INFORMATION RECORD SYSTEM

We take all reasonable steps to ensure our Information Record System is compliant and secure:

- Personal information is stored in a secure cloud facility, accessed only with an authorised log in and password.

7.2 INFORMATION SECURITY

We undertake several security measures in relation to Information Security, including:

- Staff training;
- “Clean desk” procedures;
- Need-to-know and authorisation policies;
- Just-in-time collection policies;
- Password protection;

- Policies on laptop, mobile phone and portable storage device security;
- Policy on timely culling;
- Culling procedures including shredding and secure disposal etc.

8. 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;
- When we are legally required to do so.

8.1 RELATED PURPOSE DISCLOSURES

We outsource a number of services to contracted service providers (CSPs) from time to time. Our CSPs may see some of your personal information. Typically, CSP's 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;
- Superannuation fund managers;
- A Workers' Compensation body;
- Background checking and screening agents;
- Payroll and contract management providers.

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.

8.2 CROSS-BORDER DISCLOSURES

Your personal information is not likely to be disclosed to overseas recipients. However, in the event that it is, 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 need to seek your consent to disclosure.

9. IF YOU DO NOT GIVE US ALL OR PART OF THE INFORMATION WE NEED

- We may be limited in our ability to locate suitable work for you;
- We may be limited in our ability to place you in work;
- We might decline to represent you in your search for work;
- We might decline putting you forward for particular positions.

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 while performing reference checks;
- 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 it will be observed. We do refuse access if it would breach confidentiality.

For more information about access to your information refer to our Access Policy.

For more information about applying to correct your information refer to our Correction Policy.

10.1 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.

Subject to some exceptions which are set out in the Australian Privacy Principles (APP:12) APP, you have a right to see a copy and have a copy of personal and sensitive information about you that we hold.

If you wish to exercise your rights of access and correction, you should contact our Privacy Co-ordinator, whose details are shown below. You will need to be able to verify your identity. We will make every effort to respond to your access request within 10 business days of receipt of your request.

Should you be unsatisfied with respect to the handling of your personal or sensitive information, you can make a complaint to the Office of the Australian Information Commissioner OAIC Complaint.

10.2 CORRECTION POLICY

Subject to some exceptions, which are set out in the Australian Privacy Principles (APP:13) APP, you have a right to correct personal and sensitive information about you that we hold.

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. You will need to verify your identity. We will make every effort to respond to your access request within 10 business days of receipt of your request.

If you are able to establish that personal or sensitive information that we hold about you is not accurate, complete and up to date, we will take reasonable steps to correct that information, so it is accurate, complete and up to date.

If we are unable to agree that personal or sensitive information that we hold about you is accurate, complete and up to date, you may ask us to attach information by way of a statement by you, which claims that particular information is not accurate, complete and up to date.

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 have 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 take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purposes for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Should you be unsatisfied with respect to the handling of your personal or sensitive information, you can make a complaint to the Office of the Australian Information Commissioner OAIC Complaint.

11. COMPLAINTS

We are committed to abiding by the terms set out in this document. However, if something does go wrong and you have a privacy related complaint, please let us know as it gives us the opportunity to address the problem.

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

For more information about our Complaints Procedure, see below.

11.1 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 Co-ordinator, Caron Savian, caron.savian@cmr.com.au.

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

Complaints may also be made to the RCSA, the industry association of which we are a member RCSA Complaint. The 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 Associate 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 Association's members.

11.2 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 inquiries of people who can assist us to establish what has happened and why;
- We will require a reasonable time (usually 30 days) to respond;
- If the complaint can be resolved in accordance with the procedures for access and correction, we will suggest these to you as a possible solution;

- 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 OAIC Complaints.

12. CHANGES TO OUR PRIVACY POLICY AND COLLECTION STATEMENT

If at any time our policy changes, the updated details will be available on our website for your perusal. If at any time you have a question or concern regarding Cornerstone Medical Recruitment and privacy, please contact us.

13. NOTIFIABLE DATA BREACHES SCHEME

Cornerstone Medical Recruitment Pty Ltd takes reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

A data breach is unauthorised access to or unauthorised disclosure of your personal information, or a loss of your personal information, that Cornerstone Medical Recruitment Pty Ltd holds.

Please refer to Appendix A which outlines our Policy in the event of a breach.

14. TAX FILE NUMBERS

Cornerstone Medical Recruitment Pty Ltd is a National On Hire Employer and as such collects personal information such as Tax File Numbers (TFN's). As a result of this we are considered under the Privacy Act 1988 to be a 'lawful Tax File Number Recipient' and as such comply with the *TFN Rule*.

Please refer to *Appendix B*.

15. HOW TO CONTACT US

If you wish to contact us about your personal information you should contact Cornerstone Medical Recruitment, on 1300 267 300, during normal office hours, which are Monday to Friday 8.00am – 5.00pm.

If you need to contact us about your personal or sensitive information urgently outside normal office hours, you should email us on info@cmr.com.au.

APPENDIX A

A Data breach occurs when personal information held by Cornerstone Medical Recruitment Pty Ltd is subject to unauthorised access or disclosure or is lost.

We collect personal information in relation to candidates and employees. We are aware that this information can become personal information when it is combined with other information if this combination of information results in an individual becoming 'reasonably identifiable' as a result of the combination.

Personal Information is information about an identified individual, or an individual who is reasonably identified. Personal Information is defined by the *Privacy Act 1988* as:

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) Whether the information or opinion is true or not; and*
- (b) Whether the information or opinion is recorded in a material form or not.*

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Example of a data breach:

- Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.
- Unauthorised access to personal information by an employee.
- Inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person.
- Disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

We minimise the risk of harm to an individual as a result of a data breach by following and upholding the thirteen Australian Privacy Principles (APPs) as per *the Privacy Act 1988*.

A Data Breach will have occurred when the following are met:

- There is unauthorised access or disclosure of personal information held by CMR (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- It is likely to result in serious harm to any of the individuals to whom the information relates.
- CMR has been unable to prevent the likely risk of serious harm with remedial action.

To reduce the risk of harm we will notify the individual of the data breach if it has been assessed that serious harm is likely, to enable the individual to take steps to reduce their risk of harm. For example, changing their passwords or being aware of the scam or identity fraud.

If a suspected or known data breach has occurred our response plan will be actioned. The Data Breach Response Plan consists of four (4) sections being **Contain**, **Assess**, **Notify** and **Review** as detailed below.

DATA BREACH RESPONSE PLAN

1: Contain

We will take immediate steps to contain the suspected or known breach where possible. Immediate shutdown of further access to the affected personal information will be actioned as soon as the breach is recognised.

2: Assess

We will assess whether the data breach is likely to result in **serious harm** to any individuals whose information was involved in the breach. If there are reasonable grounds the breach **could** cause harm we will notify the individual. If we suspect harm could be caused, we will undertake an **assessment** to consider if **remedial action** is required.

3: Notify

We are required to notify individuals and the Commissioner about data breaches that are **likely** to result in serious harm.

We will notify individuals in the event of a data breach after an assessment has been undertaken by the Chief Operations Officer or other authorised representative of Cornerstone Medical Recruitment Pty Ltd.

Notification will ONLY be made after it has been assessed that **serious harm is likely**.

4: Review

We will undertake a review which will involve:

- A security review including a root cause analysis of the data breach
- A prevention plan to prevent similar incidents in the future
- Audits to ensure the prevention plan is implemented
- A review of policies and procedures and changes to reflect the lessons learned from the review
- Changes to employee selection and training practices
- A review of service delivery partners that were involved in the breach.

APPENDIX B

Cornerstone Medical Recruitment Pty Ltd, is a Tax File Number (TFN) Recipient. As such, we collect TFN information and are in possession of these records and control the related information.

We apply our Notifiable Data Breach Scheme Policy and Data Breach Response Plan to any suspected or known data breaches relating to TFN information.

To further protect our employee's information we have implemented the following:

- It is our Policy that TFN's are not to be released unless the following has occurred:
 - The owner of the TFN has provided CMR with written authority to release the TFN and send via email or other form of transmission
 - The Australian Taxation Office requires transmission of the TFN via our payroll system portal