Privacy Policy

1. Background

The Westmead Institute for Medical Research ABN 54 145 482 051 is a not-for-profit medical research institute dedicated to enriching the health and wellbeing of people globally by liberating them from the major disease challenges of our time. The Westmead Institute for Medical Research Foundation ABN 90 141 847 634 raises funds for this research.

The Westmead Institute for Medical Research and The Westmead Institute for Medical Research Foundation (collectively referred to as **WIMR**) are closely affiliated with the University of Sydney Faculty of Medicine and Health, Westmead Hospital, other members of the Westmead Research Hub and Westmead Health Precinct, other bodies from time to time and the wider health system (collectively referred to as the **Affiliates**).

The medical research conducted at WIMR's premises using its facilities is predominately conducted and controlled by persons and bodies related to the Affiliates. WIMR may itself conduct a limited number of medical research projects from time to time.

2. Purpose

This Privacy Policy (**Policy**) sets out how WIMR manages the collection, use, disclosure and handling of, or otherwise processes, personal information in accordance with the Australian Privacy Principles (**APPs**) set out in the *Privacy Act 1988* (Cth), the *Health Records and Information Privacy Act 2002* (NSW), and regulations and guidelines issued pursuant to those laws.

3. Scope

This Policy applies to WIMR and participants in medical research projects conducted by WIMR, donors, supporters, applicants, students, non-employee members of WIMR, referees, contractors, suppliers and other individuals who WIMR deals with or who interact with WIMR (**you**).

This Policy does not apply to the personal information of current and former employees of WIMR.

4. Definitions

In this Policy the following terms have the following definitions:

"**Health information**" means personal information about an individual's health or disability. It includes information or opinion about an individual's illness, injury or disability.

"**non-employee members of WIMR**" include:

- any person employed by an external entity who is formally engaged to undertake research or its support at WIMR; and
- Hub Equipment / Building Users, these being persons who are not WIMR employees, but who require access to the equipment located in WIMR, or meetings rooms in restricted areas.

"**Personal information**" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Personal information includes information collected about an individual such as their name, address, bank account details and credit card information, photos, information about opinions and likes/dislikes,

and can also be captured in business records generated by the business. Information about a person who is deceased and de-identified information are not personal information.

"**Sensitive information**" means a category of personal information which includes an individual's racial or ethnic origin, health or medical information, political opinion, membership information relating to a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, criminal record, and genetic information. In this Policy information, which has potentially serious consequences if misused, such as a passport, visa or salary information, is treated in the same manner as sensitive information.

5. Types of personal information that we collect and hold

WIMR may collect and hold personal information that is reasonably necessary for the proper performance of our activities or functions as a medical research institute and charitable foundation.

The type of personal information that WIMR collects and holds is likely to differ depending on the individual's relationship with WIMR.

5.1 Research Participants

The following types of personal information, including sensitive and health information, may be collected by WIMR for the purpose of recording your involvement in a project, to process the results of a project and to contact you regarding participation in future projects:

- information including your name, address, email address, contact telephone number, gender, racial or ethnic origin, age and emergency contact;
- information including your medical history including where relevant your family medical history, Medicare number and private health insurance;
- information including the name of any care provider, medical service provider or medical specialist and copies of any referrals or reports from those parties;
- a copy of test results and samples; and
- biological samples.

5.2 Supporters / Donors

The following types of personal information may be collected by WIMR for the purpose of sending you a receipt or our fundraising activities:

- information including your name, address, email address, contact telephone number, gender and age;
- your research areas of interest;
- your event attendance history; and
- payment information, including your credit card details.

5.3 Applicants

The following types of personal information may be collected by WIMR for the purpose of our recruitment functions:

- information including your name, address, email address, contact telephone number, gender, age, employment history, educational history including academic transcript, references, resume and emergency contact;
- information submitted and obtained from the applicant and other sources (e.g. referees) in connection with applications for work;
- information about personality, character, skills, qualifications and experience;
- information about work entitlement and ability to undertake specific types of work;

- information about health status and ability to undertake specific types of work;
- work performance information;
- information about incidents in the workplace;
- information submitted and obtained in relation to absences from work due to leave, illness or other causes;
- bank details and tax file number;
- information required to ascertain an applicant's right to work in Australia (i.e. confirmation of citizenship, residency or visa status); and
- proof of identification from an applicant including copies of their passport, visa, driver's license or any other relevant licences.

For applicants who apply for employment with WIMR, we may also collect the following sensitive and health information from you:

- information regarding your medical history where it relates to your ability to perform the inherent requirements of the position you are applying for; and
- information required to undertake criminal history checks and obtain criminal history records, working with children checks etc.

5.4 Students and other non-employee members of WIMR

The following types of personal information may be collected by WIMR from these persons for purposes including the assessment of applications to undertake research projects with WIMR or for scholarships and grants:

- information including your name, address, email address, contact telephone number, gender, age, employment history, educational history including academic transcript, references, resume and emergency contact;
- information submitted and obtained from the student and other sources (e.g. referees) in connection with the application;
- information about personality, character, skills, qualifications and experience;
- information about your vaccination history;
- bank details and tax file number;
- information required to ascertain an applicant's right to study and/or work in Australia (i.e. confirmation of citizenship, residency or visa status); and
- proof of identification from an applicant including copies of their passport, visa, driver's license or any other relevant licences.

5.5 Referees

The following types of personal information may be collected by WIMR for the purpose of determining the suitability of the applicant:

- information including your name, address, email address, contact telephone number, gender and age;
- information about your work position and/or educational history and authority to give a reference;
- opinions regarding the applicant's character and work performance or work environment; and
- information in support of those opinions, sometimes involving the referee's own knowledge and experience of having worked with the applicant.

5.6 Others

For other individuals that WIMR deals with such as suppliers or contractors, we may collect information including name, address, email address, contact telephone number, position, ABN, business records, billing information, licence or registration numbers, bank details, information about the goods and services supplied and any other personal information you choose to provide us that is reasonably

necessary for the proper performance of our activities or functions as a medical research institute and charitable foundation.

5.7 Visitors to our Website

When you visit our website to read, browse or download information, our system may record information such as browser type, operating system, the date and time you visit the website, the pages accessed, time spent and any information downloaded. This information is used to analyse how people use our website so that we can improve our offerings.

Like many other websites, our website may use an internet browser feature from time to time called 'cookies'. A cookie is a small data file that may be placed on a web user's computer (usually in the browser software folder) the first time that a computer visits a website that operates cookies. Cookies by themselves cannot be used to personally identify you – they only identify the computer used to visit our website and help us maintain the continuity of your browsing session by remembering your preferences for when you return. You can configure your web browsing software to reject cookies, however this may limit the functionality of our website or prevent you from accessing some parts of our website.

6. How we collect your personal information

WIMR usually collects personal information directly from you when you have contacted WIMR in person, over the phone, via email or the internet. However, the means by which we will generally collect your personal information are likely to differ depending on your relationship with WIMR.

6.1 Research Participants

We collect personal information from you directly when you fill in the applicable consent form to participate in a medical research project. We may also collect information from other third parties, such as medical providers, with your consent.

Generally the personal information we collect (by consent) is de-identified and stored in a secure area on the University of Sydney's research data storage platform. Access to this information is limited to authorised WIMR researchers.

6.2 Supporters / Donors

We may collect personal information from you directly when you fill out and submit one of our donation forms, when you donate at an event or any other information in connection with you contacting WIMR in order to donate or support our research activities.

6.3 Applicants / Students

We may collect personal information from you directly when you fill out and submit one of our application forms or any other information in connection with your application to us for work or to be involved in a research project. Personal information about applicants and students is also collected when:

- we receive or give any reference about you;
- we receive results of inquiries that we might make of your former employers, work colleagues, professional associations or registration body;
- we receive the results of any competency, psychometric, or medical test;
- we receive performance feedback;
- we receive any complaint from or about you in the workplace;
- we receive any information about a workplace accident in which you are involved;
- we receive any information about any insurance investigation, litigation, registration or professional disciplinary matter, criminal matter, inquest or inquiry in which you are involved; or

- you provide us with any additional information about you.

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. We collect personal information about you from publicly available sources for inclusion in our records only as is reasonably necessary for the performance of our recruitment functions, and this information is managed in accordance with this Policy.

6.4 Referees

We may collect personal information when you provide it to us:

- in the course of our obtaining a reference for an applicant or student with you and when we are checking information that we obtain from you about an applicant or student;
- for business or business related social purposes; and
- electronically through our telecommunications and technology systems.

6.5 Others

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

- sign up to be on an email list such as for our newsletter;
- make a written online enquiry or email us through our website;
- submit a resume by email or through our website;
- make a job application to us through an external job board or website; and
- follow and communicate with us via social media such as LinkedIn, Facebook and Twitter.

6.6 Unsolicited Information

From time to time, WIMR may also receive unsolicited information, being information that we have not taken active steps to collect. Examples include misdirected mail, unsolicited employment applications and promotional flyers containing personal information.

When we receive such information, we will decide within a reasonable period whether we could have collected it pursuant to the requirements in the APPs. If we determine that we could not have collected the information, we will destroy or de-identify it as soon as practicable. Alternatively, if we determine that we could not have collected the information and wish to retain it, we will deal with this information in accordance with our obligations under the APPs.

7. How we hold your personal information

When your personal information is collected it will be held in our 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.

7.1 Our System

Personal information you provide to us is stored in electronic records and systems as follows:

- personal information collected for medical research is stored on a locally based server or a cloud based server; and
- personal information collected for administration purposes is stored on a cloud based server.

In both cases, access to the information is restricted to those who have a business or legal need to know the information, and accessible through the use of an individual log-in credentials, which are confidential to the individual. A systems administrator also has access to the information.

Your information may also be securely stored in hard copy in a lockable filing system until such time as it is digitised and that information is filed in our electronic system. When this occurs, the hard copy document/s are subsequently destroyed in a timely manner.

Other personal information collected from research participants which is identifiable data (i.e. it is not de-identified) is stored on a secure platform at WIMR, and access is limited to a small number of authorised researchers.

7.2 Information Security

We will take all reasonable steps to ensure the personal information you provide us remains secure and confidential and is only used as provided for in this Policy in the performance of our functions or activities as a medical research institute and charitable foundation.

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

- training of employees, students and researchers;
- password-protection of cloud-based database and document storage system, together with firewalls, user identifiers and passwords to control access;
- secure office premises with restricted access;
- need-to-know and authorisation policies;
- policies on laptop, mobile phone and portable storage device security; and
- document culling procedures including shredding and secure disposal.

7.3 Third party websites

WIMR's website may contain links to other websites that are not owned or controlled by WIMR. We are not responsible for the privacy practices or policies of those websites.

8. How your personal information is disclosed

This section deals with our disclosure policies. Personal Information that we hold about you is only disclosed for the primary and related purposes for which it was collected.

8.1 General (Primary) Disclosures

We may disclose your personal information for any of the purposes for which it is primarily held or for a related purpose where lawfully permitted. We may also disclose your personal information where we are under a legal duty to do so, including circumstances where we are under a contractual duty to disclose information.

Disclosure of personal information will usually be:

- internally and to our related entities;
- to our Affiliates; and
- to referees for suitability and screening purposes.

8.2 Related Purpose Disclosures

In addition to disclosures for general purposes, we may also disclose your personal information for a range of related purposes. 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;
- IT contractors;

- financial service providers;
- database designers and internet service suppliers;
- legal and other professional advisors;
- insurance brokers, loss assessors and underwriters;
- Government bodies as required by law; and
- 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.

8.3 Cross-Border Disclosures

Depending on the circumstances and the location where a medical research program is being conducted or coordinated, there may be instances where disclose of personal information involves a cross-border disclosure. In this regard, our programs are occasionally internationally based and our staff, agents, service providers, collaborators and research partners may be located overseas.

As a general principle, we will only disclose personal information to an overseas recipient where we reasonably believe that the recipient is subject to laws that are substantially similar to the APPs, or where cross boarder disclosure is permitted by law. In the event that cross border disclosure of personal information is required we will seek to obtain your informed consent.

9. Direct Marketing

We directly market to supporters and donors using a variety of methods including email, social media (including Facebook, Twitter and LinkedIn), phone and print.

WIRM will not use your personal information for direct marketing purposes unless you have provided express consent, or your consent can reasonably be implied from the circumstances in which we collected the information.

If WIMR sends you marketing material we will ensure that you can 'opt-out' of receiving any future marketing material. In relation to direct marketing via electronic means, such as email, we comply with the *Spam Act 2003* (Cth) and in relation to telephone marketing we comply with the *Do Not Call Register Act 2006* (Cth).

10. Access and Correction

You have a right to access and correct personal information under the APPs.

10.1 Access

You can gain access to the personal information that we hold about you subject to the exceptions that are set out in privacy law.

One exception is where giving access would have an unreasonable impact on the privacy of other individuals. This exception applies to evaluative opinion material obtained confidentially in the course of our performing reference checks, where access that would impact on the privacy rights of the individual who provided the reference confidentially. In these circumstances, we may refuse access if the evaluative material contained in references would breach any confidentiality obligation we have with the referee.

10.2 Correction

You can ask us to correct your personal information that we hold about you if it is inaccurate, out of date, incomplete, irrelevant or misleading. We will take reasonable steps under the circumstances to correct that information.

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 reasonable steps (if any) in the circumstances to give that notification unless it is impracticable or unlawful to do so.

10.3 Timeframe

You should also anticipate that it may take a little time to process your application for access or correction as there may be a need to retrieve information from storage and review information in order to determine what information may be corrected. We will generally respond to your request for access within five (5) working days.

10.4 Refusal

If we refuse to give access to, or correct, your personal information as requested by you, we will give you a written notice that sets out:

- the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal.

If we refuse to correct your personal information, you may ask us to place with the information a statement that the information is contested as being inaccurate, out of date, incomplete, irrelevant or misleading, and we will take such reasonable steps under the circumstances to associate the statement with your information.

10.5 Cost

Depending on the nature of the request, we may need to charge you for providing access to the personal information. These charges will be reasonable, and we will let you know if a charge will apply before proceeding with the request.

We will not charge you for making the request to correct your information, correcting the information, or associating a statement.

11. Anonymity

Where lawful and practical, you will be given the option to deal with us without identifying yourself or by using a pseudonym (e.g. when inquiring about the activities that WIMR or the Affiliates undertake).

12. Complaints

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

12.1 How to complain

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 please contact:

- By post, addressed to:

Chief Operations Officer
Westmead Institute for Medical Research
PO Box 412
WESTMEAD NSW 2145

- By email, at hr@westmeadinstitute.org.au
- By phone, on 02 8627 3000

You can also make complaints to the Office of the Australian Information Commissioner or the NSW Information and Privacy Commission ()www.ipc.nsw.gov.au).

12.2 How your Complaint will be Handled

When we receive a complaint:

- we will take reasonable 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 established what has happened and why;
- we will require a reasonable time (usually 30 days) to respond;
- if the complaint can be resolved by procedures for access and correction, we will suggest these to you as possible solutions; and
- 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 take your complaint the Office of the Australian Information Commissioner.

13. Amendments to this Policy

This Policy may change over time in light of changes to privacy laws, technology and operational practices.

If you use our website regularly or conduct transactions with us that involve us collecting your personal information, it is important that you check this Policy regularly to ensure that you are kept informed on an updated basis of the extent of any consent, authorisation or permission you might give.