

Privacy Policy

1. APPLICATION

- 1.1 This Policy applies to any information collected, obtained, held or disclosed by HMRI Directors, officers, employees, volunteers and HMRI Affiliates, (collectively HMRI Representatives) in the course of carrying out activities on behalf of HMRI.
- 1.2 The Policy applies to all visitors to the HMRI website or any social media platform controlled by HMRI and other persons who interact with HMRI or whose personal information HMRI may deal with in carrying out its activities.
- 1.3 To the extent that this policy relates to activities or conduct of non-employees of HMRI, the policy is intended to supplement and not alter any policy of the employer. In the event of any inconsistency between this policy and the policy of an individual's employer, the employer's policy should take precedence.

2. INTRODUCTION

- 2.1 HMRI is committed to handling personal information (including health and other sensitive information) respectfully and in accordance with applicable laws and HMRI policies and procedures including the Technology and Information Security Policy.
- 2.2 The treatment of personal information of HMRI Directors and Officers, employees, affiliates and volunteers is also guided by the HMRI Code of Conduct.
- 2.3 HMRI collects, holds, uses and discloses personal information to carry out functions or activities in accordance with the Privacy Act 1988 (Cth) (Privacy Act), the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) the Health Records and Information Privacy Act 200 (HRIPA) and the National Health and Medical Research Council Guidelines (Privacy Act ss 95 & 95A).
- 2.4 The specific legal obligations of HMRI when collecting and handling personal information are outlined in the Privacy Act and in particular in the Australian Privacy Principles (APPs) found in that Act.

3. POLICY INTENT

- 3.1 This Policy advises persons whose personal information HMRI collects, holds, uses and discloses and visitors to HMRI's website and social media platforms, of how their personal information is collected and managed.
- 3.2 This Policy, along with HMRI's Technology and Information Security Policy and Privacy Disclosures, informs HMRI Representatives of their responsibilities relating to the handling of personal information.

4. COLLECTION AND USE OF PERSONAL INFORMATION

- 4.1 HMRI will only collect personal information (including sensitive information) which is reasonably necessary for HMRI's functions or activities, from individuals who consent to the collection or from a third party who is authorised to provide HMRI with the information.
- 4.2 HMRI may collect information from individuals which contains health information or other sensitive information with consent.
- 4.3 HMRI generally collects personal information (including sensitive information) from you or your authorised representative when you provide it to us including through email or online forms, when it is part of a data set provided by a healthcare provider or service (consistent with an approved ethics protocol) or through our website.
- 4.4 HMRI will also collect your personal information when you apply for a job at HMRI or report any matter to HMRI for investigation.
- 4.5 HMRI may collect information that you provide to us when signing up to mailing lists and registering for our events, or when submitting feedback on your experience with our website.
- 4.6 HMRI sometimes collects personal information from a third party or a publicly available source for marketing or fundraising purposes, or in connection with conducting research, analysis or advisory services.
- 4.7 Personal information may also be collected through our websites and social networking services such as Linked in, Facebook, Twitter and Instagram. We use this information to improve our website and consider feedback from the community.

5. VISITORS TO THE HMRI WEBSITE FROM THE EUROPEAN ECONOMIC AREA

- 5.1 If you are an individual in the European Economic Area (EEA), you may have the right to request the restriction of, or objection to, the processing of your personal information, and the portability and erasure of information under the General Data Protection Regulation (GDPR).
- 5.2 If you would like to request an amendment to any personal information collected by HMRI relating to you, pursuant to the GDPR, you can contact us - see 'Contact us' below.

6. HOLDING PERSONAL INFORMATION (STORAGE AND SECURITY)

- 6.1 HMRI uses physical security and electronic measures to ensure that personal information is protected from misuse, interference and loss; and from unauthorised access, modification and disclosure.

- 6.2 Personal information collected by HMRI in the course of its activities or for the HMRI Research Register is held on our cloud storage, on servers located in Australia. We have controls over any personal information held on our cloud, and the information is handled in accordance with the Australian Privacy Principles.
- 6.3 HMRI ensures that personal information is not kept for longer than necessary to comply with laws, consents and protocols and that information authorised to be destroyed is destroyed securely.
- 6.4 Donations and registrations made on the HMRI website use encryption methods and credit card data is stored using systems compliant with the Payment Card Industry Data Security Standard.
- 6.5 HMRI holds licences to OpenSpecimen and Redcap platforms which are managed by the HMRI ICT team and hosted in Australia. Personal information collected by Affiliated Researchers may be uploaded or inputted into databases using HMRI instances of OpenSpecimen and/or Redcap with access subject to the HMRI information access procedures and any relevant consents and/or ethics protocols.

7 USE AND DISCLOSURE OF PERSONAL INFORMATION

- 7.1 Personal information will be used by authorised employees carrying out HMRI activities for the purpose for which the information was collected. In some circumstances personal information may be used for a secondary purpose related to the purpose for which the information was given which you would reasonably expect.
- 7.2 HMRI will only disclose sensitive information for the purposes for which it was given to us; for directly related purposes an individual would reasonably expect; when an individual has consented; in accordance with approved protocols, ethics or other relevant approvals; in aggregated and/or deidentified formats; or when HMRI is entitled or required to do so by law.
- 7.3 HMRI uses a number of service providers to whom we disclose personal information. These include providers that host our website servers, develop web-based platforms, manage our IT and facilitate fundraising activities. HMRI enters into contracts with the service providers to ensure compliance with the APPs.
- 7.4 From time to time HMRI may use systems located outside of Australia to manage data for operational reasons. All such data is deidentified. Examples of data which may be held in overseas locations are Google analytics data regarding browsing and billing data.

8 MARKETING RESEARCH AND MARKETING

- 8.1 HMRI may, from time to time, use name and address details (including email addresses) to communicate with individuals and organisations regarding fundraising -

including providing information on how donations have been spent and seeking support for future HMRI research and support activities.

8.2 From time to time, HMRI may provide name and address details of an individual or organisation, to another organisation who may wish to communicate with that individual or organisation to provide information that may be of interest to them (for example like-minded charities).

9 ACCESS AND COMPLAINTS RELATING TO PERSONAL INFORMATION

9.1 You have the right to ask for access to personal information that we hold about you, and ask that we correct that personal information. If you ask, we must give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to.

9.2 If you would like to prevent HMRI from providing name and address details to any other organisation you can contact us - see 'Contact us' below. Alternatively, HMRI will provide an opportunity to "OPT OUT" of communications by following the instructions in our email or print communications.

Contact Us

If you wish to access, correct or complain to us about how we have handled your personal information you should first notify us in writing. You can contact us by:

Website: hmri.org.au
Email: privacy@hmri.org.au
Telephone: Head of Legal and Risk
Post: Head of Legal and Risk
Hunter Medical Research Institute
1 Kookaburra Circuit
New Lambton Heights NSW 2305

DEFINITIONS

HMRI ICT means all technology related systems owned or managed by HMRI, both hardware and software.

Personal information means any 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' (s 6(1)).

Sensitive information means health information, genetic information (that is not otherwise health information), biometric information that is to be used for the purpose of automated

biometric verification or biometric identification, or biometric templates or information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions or membership of a political association;
- philosophical beliefs, religious beliefs or affiliations;
- membership of a professional or trade association or union;
- sexual orientation or practices; or
- criminal record.

RELATED DOCUMENTS

- Code of Conduct Policy
- Technology and Information Security Policy
- Privacy Disclosures

VERSION CONTROL

Approval date	Effective date	Version
11/04/2024 Board	18.07.24	20V1