PRIVACY POLICY

1. INTRODUCTION

The George Institute for Global Health, together with its subsidiary and associated companies worldwide (**The George Institute** or **TGI**), is committed to ensuring the privacy and confidentiality of Personal Information it receives. Equally, our people (employees, representatives and associates) share this commitment.

This Policy (and the underlying practices and processes employed at The George Institute) are designed in accordance with the Australian Privacy Principles (**APPs**) of the Australian *Privacy Act 1988 (Cth)*, the *Health Records and Information Privacy Act 2002 (NSW)*, and regulations and guidelines issued pursuant to those Acts (**Privacy Laws**).

The George Institute has adopted the APPs as the minimum standard across all of its offices worldwide. However, if regional legislation requires a higher standard, then regional offices must abide by that higher standard. The EU General Data Protection Regulation ((EU) 2016/679) (**GDPR**) is an example of such a higher standard. Where TGI processes Personal Information of individuals located within the European Union, or with the help of or on behalf of an EU entity (regardless of where the relevant individuals are located) additional requirements under GDPR may apply.

The George Institute also applies and follows the *ICH Guidelines for Good Clinical Practice* with respect to the use, protection and security of Health Information collected, as well as guidelines issued by the National Health and Medical Research Council of Australia (**NHMRC**) in respect of Health Information that may be accessed in the conduct of research.

2. SCOPE

All executive, regional and divisional directors, heads of business and senior managers must ensure that this Policy is considered and applied to all processes and standard operating procedures applicable to their area of responsibility, and staff within their area(s) are advised of and trained in the practical applications of this Policy.

This Policy applies to all permanent and temporary staff of The George Institute, and any consultants, students or other persons working at TGI offices (collectively, **TGI staff**).

Any questions in respect of this Policy and/or Privacy Laws, or any privacy complaints, should be referred to the Privacy Officer – privacy@georgeinstitute.org or GCprivacy@georgeclinical.com (**George Clinical** companies and branches only).

DEFINITIONS

In this Policy, the following terms are used:

- **Health Information** – Personal Information that is information or an opinion about: (i) the physical or mental health or a disability of an individual; (ii) an individual's express wishes about the future provision of Health Services to that individual; (iii) a Health Service provided (or to be

provided) to an individual; (iv) other Personal Information collected to provide (or in providing) a Health Service; (v) other Personal Information about an individual collected in connection with the donation (or intended donation) of an individual's body parts, organs or body substances; (vi) other Personal Information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual; and (viii) healthcare identifiers.

- **Health Service** includes: medical, hospital, nursing and midwifery services; dental services; mental health services; pharmaceutical services; ambulance services; community health services; health education services; welfare services necessary to implement any before mentioned services; services provided in connection with Aboriginal and Torres Strait Islander health practices and medical radiation practices; Chinese medicine, chiropractic, occupational therapy, optometry, osteopathy, physiotherapy, podiatry and psychology services; optical dispensing, dietitian, massage therapy, naturopathy, acupuncture, speech therapy, audiology and audiometry services; and services provided in other alternative health care fields in the course of providing health care.
- **Personal Information** – Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.
- **Sensitive Information** – Personal Information that is information or an opinion about an individual's racial or ethnic origin, political opinions, memberships (political association, professional or trade association, or trade union), religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, and/or criminal record. Also includes health or genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.
- **Industry Rules** – Rules established by competent health or medical bodies that deal with obligations of professional confidentiality.

3. THE AUSTRALIAN PRIVACY PRINCIPLES (APPs)

3.1 APP 1 – Open and transparent management of Personal Information

Principle

TGI will manage Personal Information in an open and transparent manner by:

- implementing practices, procedures and systems to ensure compliance with the APPs, including a process to deal with any inquiries or complaints from individuals about TGI's compliance with the APPs;
- having a privacy policy, which describes TGI's management of Personal Information (*e.g. collection, use, storage and disclosure*) and how an individual may contact TGI to request access to, or correction of, their Personal Information which is held by TGI; and
- making such Policy (as updated from time to time) readily available on its public website or in hard-copy form available on request.

Application

TGI's standard operating procedures are drafted to comply with this Principle.

This Policy and standard-form privacy statements, disclosure and consent forms, and operational checklists aid TGI staff in compliance with this Principle. Training programs are made available to staff.

TGI has a designated Privacy Officer, who is authorised to deal with any inquiries or complaints. Contact details are provided in this Policy and on TGI's public website.

3.2 APP 2 – Anonymity and pseudonymity

Principle

TGI will give individuals (when dealing with TGI in relation to a particular matter) the option of not identifying themselves or using a pseudonym, unless it is impracticable or Australian law or a court/tribunal order provides otherwise.

Application

For most dealings with TGI, individuals will need to provide at least their name and contact information to enable TGI to assist with their query.

In respect of TGI's research activities, Personal Information will most likely be required, and in the majority of cases some Sensitive Information (e.g. Health Information).

If TGI conducts a general survey not requiring Personal Information, then the option of anonymity and pseudonymity will be offered.

Managers are required to consider this principle when establishing, reviewing, and authorising standard operating procedures and protocols.

3.3 APP 3 – Collection of solicited Personal Information

Principle

TGI will only collect Personal Information (that is reasonably necessary for its functions or activities) by lawful and fair means, and from the individual concerned (or from another person if it is unreasonable or impracticable to collect from the individual concerned).

TGI will only collect Sensitive Information, including Health Information (that is reasonably necessary for its functions or activities) with the consent of the individual concerned, unless collection is authorised by law, a permitted general situation or permitted health situation exists, or collection is required under a court/tribunal order.

Permitted general situation

Under Privacy Laws, TGI may collect Sensitive Information (including Health Information) without individual consent in the following scenarios:

- It is unreasonable or impracticable to obtain an individual's consent, and the collection of such individual's information is reasonably necessary to lessen or prevent a serious threat to the life, the health or safety of an individual, or to public health or safety.
- An unlawful activity or act of serious misconduct is suspected, and the collection is reasonably necessary to take appropriate action.
- The collection is reasonably necessary to assist another in the location of a person who has been reported as missing.
- The collection is reasonably necessary for the establishment, exercise or defence of a legal or

equitable claim.

- The collection is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Permitted health situation

Under Privacy Laws, TGI may collect Health Information without individual consent:

- to provide a Health Service to the individual, provided such collection is in accordance with Australian law and Industry Rules; or
- it is necessary for research relevant to public health or public safety, or for the compilation or analysis of statistics relevant to public health or public safety, or for the management, funding or monitoring of a health service (each a **Permitted Purpose**), provided that the Permitted Purpose cannot be served by the collection of de-identified information, it is impracticable to obtain the consent of the individual concerned, and collection is in accordance with Australian law and Industry Rules.

Application

With respect to the collection of Health Information, TGI follows the *ICH Guidelines for Good Clinical Practice*, as well as relevant guidelines, such as those issued by the NHMRC (and other jurisdictional requirements in respect of overseas research).Personal Information and Sensitive Information (including Health Information) is typically collected for the stated purpose(s) of the particular research. Individuals participating in a research study are provided with information about the collection of their information (amongst other things), and are required to sign an appropriate participant information and consent form.

TGI's standard operating procedures are drafted to comply with this Principle. This Policy and standard-form privacy statements, disclosure and consent forms, and operational checklists aid TGI staff in compliance with this Principle. Training programs are made available to staff.

3.4 APP 4 – Dealing with unsolicited Personal Information

Principle

When receiving unsolicited Personal Information, TGI will confirm whether or not such Personal Information could have been collected under Privacy Laws (i.e. as if TGI had solicited the Personal Information), and if not TGI will destroy or de-identify the Personal Information as soon as practicable (provided it is lawful and reasonable to do so).

Application

TGI may, on rare occasions, receive unsolicited Personal Information, which will be dealt with according to this principle.

TGI's standard operating procedures are drafted to comply with this Principle.

3.5 APP 5 – Notification of the collection of Personal Information

Principle

Before collecting an individual's Personal Information (or at collection, or as soon as practicable after collection), TGI will:

- notify such individual of the collection, and the circumstances, the authority, and purposes of

such collection; and

- provide a document or statement which sets out the required privacy disclosures – e.g. TGI's details, how TGI collects and manages such Personal Information, and how an individual can contact TGI to access or correct his/her Personal Information or make a complaint.

Application

This Policy includes a 'Privacy Policy – Public Statement' which provides the required privacy disclosures in a general form, and which is available on TGI's corporate website. A similar statement is available on George Clinical's corporate website.

Each research study being managed or conducted by TGI that involves the collection of Personal Information will include the required privacy disclosures specific to that study.

TGI's standard operating procedures are drafted to comply with this Principle.

3.6 APP 6 - Use or disclosure of Personal Information

Principle

TGI will only use or disclose an individual's Personal Information for the purpose(s) for which it was collected (*i.e. as set out in the information/consent document/form given to the individual*), for a related purpose (*and the individual would reasonably expect his/her information to be used or disclosed for this purpose*), for a permitted general situation or permitted health situation, or as otherwise consented to by the individual, or as permitted by Australian law or court/tribunal order.

TGI will only use or disclose an individual's Sensitive Information (including Health Information) for the purpose(s) for which it was collected (*i.e. as set out in the information/consent document/form given to the individual*), a directly-related purpose (*and the individual would reasonably expect his/her information to be used or disclosed for this purpose*), for a permitted general situation or permitted health situation, or as otherwise consented to by the individual, or as permitted by law or court/tribunal order.

Permitted general situation (as applicable to TGI)

Under Privacy Laws, TGI may use or disclose Personal Information if:

- it is reasonably necessary to lessen or prevent a serious threat to the life, the health or safety of an individual, or to public health or safety (and it is unreasonable or impracticable to obtain the individual's consent);
- unlawful activity or serious misconduct is suspected;
- it is reasonably necessary to assist in locating a person who has been reported as missing;
- it is reasonably necessary to establish, exercise or defend a legal or equitable claim; or
- it is reasonably necessary to pursue confidential alternative dispute resolution.

Permitted health situation (as applicable TGI)

Under Privacy Laws, TGI may use or disclose Health Information which is necessary for research (or the compilation or analysis of statistics) relevant to public health or public safety, if it is impracticable to obtain the consent of the individual(s) concerned, and the use and disclosure is conducted in accordance with relevant guidelines, such as those issued by the NHMRC. Further, in the case of disclosure, TGI must reasonably believe the recipient will not disclose the Health Information.

Application

Whenever possible, TGI will remove, redact or de-identify Personal Information prior to a permitted disclosure (i.e. under this Principle or an exception under law).

TGI's standard operating procedures are drafted to comply with this Principle.

Despite the use and disclosure exemptions listed above, ethics committee approvals may be required prior to the use or disclosure of any Health Information (as per NHMRC Guidelines).

3.7 APP 7 – Direct marketing

Principle

TGI will not use or disclose Personal Information for the purpose of direct marketing, unless otherwise permitted by Australian law.

TGI will not use or disclose Sensitive Information (including Health Information) for the purpose of direct marketing without the consent of the individual concerned.

Permitted exception

- Personal Information (other than Sensitive Information) may be used or disclosed for the purpose of direct marketing if such information was collected from the individual (and he/she would reasonably expect his/her information to be used for the purpose of direct marketing), and TGI provides an easy 'opt-out' to not receive direct marketing communications (and he/she has not made such a request).
- Personal Information (other than Sensitive Information) may be used or disclosed for the purpose of direct marketing if such information was collected from the individual (or another person), the individual has consented that his/her information may be used/disclosed for the purpose of direct marketing (unless in the circumstances it is impracticable to obtain consent), TGI provides an easy 'opt-out' to not receive direct marketing communications (and he/she has not made such a request), and in each direct marketing communication with the individual a prominent statement is included that the individual may make a request not to receive direct marketing communications (and he/she has not made such a request).
- Sensitive Information may be used or disclosed for the purpose of direct marketing if the individual concerned has consented to that use or disclosure.

Application

Being a research organisation, TGI would not usually partake in direct marketing activities.

TGI may, from time to time, issue information about our, or our collaborators', research activities in order to promote such research activities and to obtain continued funding support. An individual may request not to receive such communications from TGI (or via a third party), and TGI will give effect to such request (within a reasonable time period).

3.8 APP 8 – Cross Border disclosure of Personal Information

Principle

As a general principle, TGI will only disclose Personal Information to an overseas recipient where it reasonably believes that the recipient is subject to laws that are substantially similar to the APPs. Nonetheless, cross boarder disclosure is permitted:

- with the informed consent from the individual(s) concerned; or
- as authorised by or under applicable law or a court/tribunal order; or
- when a permitted general situation exists.

Permitted general situation (as applicable to TGI)

Under Privacy Laws, TGI may disclose Personal Information if:

- it is reasonably necessary to lessen or prevent a serious threat to the life, the health or safety of an individual, or to public health or safety (and it is unreasonable or impracticable to obtain the individual's consent);
- unlawful activity or serious misconduct is suspected; or
- it is reasonably necessary to assist in locating a person who has been reported as missing.

Application

TGI enters into legal agreements before utilising agents, service providers and research collaborators, including those that are located outside of Australia. These agreements include standard terms to address privacy and confidentiality obligations and permitted disclosures where relevant and appropriate.

TGI's standard operating procedures are drafted to comply with this Principle.

Despite the disclosure exemptions listed above, ethics committee approvals may be required prior to the use or disclosure of any Health Information (as per NHMRC Guidelines).

3.9 APP 9 – Adoption, use or disclosure of government related identifiers

Principle

TGI will not adopt a government related identifier (**GRI**) as its own identifier of an individual unless permitted by Australian law or court/tribunal order.

TGI will not use or disclose a GRI of an individual, unless such use or disclosure is reasonably necessary to verify the identity of the individual (for the purposes of TGI's activities or functions) or to fulfil TGI's obligations to government, or is otherwise permitted by Australian law or a court/tribunal order.

Application

TGI uses formulated identification numbers that are not government identifiers.

TGI's standard operating procedures are drafted to comply with this Principle.

3.10 APP 10 – Quality of Personal Information

Principle

TGI will take such steps (if any) as are reasonable in the circumstances to ensure that the Personal Information it:

- collects is accurate, up-to-date and complete; and
- uses or discloses is (having regard to the purpose of the use or disclosure) accurate, up-to-date, complete and relevant.

Application

TGI's standard operating procedures and research protocols include controls and checks to ensure the quality of information collected.

Managers are required to consider this principle when establishing, reviewing and authorising standard operating procedures and project protocols.

TGI complies with ICH Guidelines for Good Clinical Practice.

It should be noted that Personal Information (including Health Information) collected for the purpose of a research study or program will be time specific, and after closure of the research database, Personal Information cannot be updated.

3.11 APP 11 – Security of Personal Information

Principle

TGI will take such steps as are reasonable in the circumstances to:

- protect the Personal Information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure; and
- destroy or de-identify Personal Information when it is no longer needed for any purpose, and retention is not required by Australian law or a court/tribunal order.

Application

TGI uses a range of technical and organisational security precautions to protect data and information it holds, for example:

- Our offices are restricted with security measures that include access restrictions, building and floor restrictions, office security and pass-cards, security monitoring and in some instances surveillance.
- Our data storage systems are restricted with security measures that include firewalls, access restrictions and limitations, logins and passwords, and audit trails.
- Processes exist for the storing, back-up and destruction of information and records.
- Our security procedures are continuously revised based on new technological developments.
- Research databases are restricted to the specified research staff conducting the project or study. Such information is not accessible by or provided to other staff, sponsors, or publishers of research findings.

TGI's standard operating procedures are drafted to comply with this Principle.

Managers are required to consider this principle when establishing, reviewing and authorising standard operating procedures and project protocols.

3.12 APP 12 – Access to Personal Information

Principle

TGI will give an individual access to his/her Personal Information held by TGI, unless prevented by Australian law or court/tribunal order, or giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety, or unreasonably impact the privacy of other individuals.

If reasonable and practicable, access will be given in the manner requested by the individual.

Exceptions (applicable to TGI)

Under Privacy Law, access can be denied if the request is frivolous or vexatious, if the individual is in legal dispute or negotiations with TGI, unlawful activity or serious misconduct is suspected, or giving access would prejudice the activities of an enforcement body or reveal TGI's evaluative information generated in connection with a commercially sensitive decision-making process.

Application

An individual may request access to his/her Personal Information held by TGI by following the procedure outlined in this Policy (page 15).

If access is denied, TGI will provide a written response stating the reason(s) for denying the request (to the extent that it reasonable to do so), and the process by which the individual can lodge a complaint with TGI. TGI staff may advise generally why access is denied, but should be mindful not to put the individual on notice of any legal or enforcement action (as to do so could be unlawful).

TGI will respond to requests within a reasonable period, and will not charge an individual for making a request, processing a request, or giving access to Personal Information (depending on the reasonability of the manner requested).

3.13 APP 13 – Correction of Personal Information

Principle

TGI will take such steps (if any) as are reasonable in the circumstances to correct Personal Information to ensure that (having regard to the purpose for which it is held) it is accurate, up-to-date, complete, relevant and not misleading.

Application

An individual may request correction of his/her Personal Information held by TGI by following the procedure outlined in this Policy.

On receipt of a valid request, TGI will update such Personal Information of the individual, unless it unlawful or impracticable to do so. Further, if requested by the individual, TGI may notify other persons/entities to which the Personal Information was previously disclosed. In making its decision, TGI will consider the purpose for which such Personal Information is held, the legal requirements, and the practicalities of the situation.

If correction is denied, TGI will provide a written response stating the reason(s) for declining the request (to the extent that it reasonable to do so), the process by which the individual can lodge a complaint with TGI, and that he/she can contact TGI to have his/her personal information associated (linked) with a statement that such information has been advised (on such date) as inaccurate, out of date, incomplete, irrelevant or misleading (as applicable). TGI staff may advise generally why correction is denied, but should be mindful not to put the individual on notice of any legal or enforcement action (as to do so would be unlawful).

TGI will respond to requests within a reasonable period, and will not charge an individual for making a request, processing a request, and correcting the Personal Information.

4. REVISION HISTORY

Version	Replaces	Date and Description of change / reason
5.0 (1 June 2021)	4.0	Updated Policy to follow new policy template layout and structure, and incorporated other minor edits.
4.0 (19 May 2019)	3.0	Included a reference to GDPR on page 1 of the Policy and updated the *Privacy Policy – Public Statement* to reflect the version published on TGI's website.
3.0 (16 Feb 2018)	N/A	Corrected version number and added references to related Policies, SOPs and Plans, including the *TGI Data Breach Response Plan: Personal Information,* which has been updated in accordance with the Australian *Notifiable Data Breaches Scheme (Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)), effective 22 Feb 2018
V1.0 (Sep 2014)	-	First version

5. APPROVAL

Title of Owner / Author	Marna van Zyl Digitally signed by Marna van Zyl Date: 2021.06.04 16:15:59 +10'00'
Approved by: COO / Director	Tim Regan 2021.06.04 14:37:53 +10'00'

PRIVACY POLICY – PUBLIC STATEMENT

The George Institute for Global Health, together with its subsidiaries and associated companies worldwide ("**The George Institute**", "**we**" and "**our**") is committed to handling personal information (including health and other sensitive information) in accordance with applicable privacy laws, including the Australian Privacy Principles ("**APPs**") set out in the Australian *Privacy Act 1988* (Cth), and, where relevant, the EU General Data Protection Regulation ((EU 2016/679) (**GDPR**). A reference to **personal information** includes "personal data" as defined in the GDPR.

We have adopted the APPs as the minimum standard across all of our offices worldwide. We also comply with the *ICH Guidelines for Good Clinical Practice* with respect to the use, protection and security of health information collected, as well as guidelines issued by the National Health and Medical Research Council of Australia (NHMRC) in respect of health information that may be accessed in the conduct of research.

What types of personal information do we collect and why?

We collect personal information reasonably necessary for one or more of our functions or activities as medical research organisation. The types of personal information we generally collect may include your name, date of birth, address and other contact details such as your telephone numbers and email address. Depending upon the purpose of our interaction with you, we may collect additional personal information. More details about the personal information we collect (and why) are provided below.

- ***Human Research Studies / Trials***

  We (or an approved third-party operating on our behalf) will collect personal information and health information (and at times, other sensitive information) from individuals who participate in human research studies and clinical trials undertaken by The George Institute (or our related parties, including George Clinical).

  Such information collected may include:

  - gender, nationality, heritage, and date of birth;
  - medical history and treatments;
  - Medicare number (or similar) and private health insurance information;
  - current medications and treatments;
  - health services and treatments;
  - symptoms, test results and hospital care; and
  - consequential health factors.

  The information is collected for the purposes of medical research and analysis pertaining to the research study or trial, to comply with laws and regulatory guidelines relating to medical research and clinical trials, and to substantiate the findings and publication of research results.

  We may also collect personal information of health practitioners and health providers who are involved in the care of study participants (e.g. general practitioners, physiotherapists, other healthcare service providers). Such information collected may include name, address, contact details, professional qualifications, experience, and interaction records with us (as part of the particular research study or trial). This information is collected for the purpose of administration, management and operation of The George Institute and the particular research study or trial.

  We will also collect the personal information of medical experts, researchers and other professionals advising on, overseeing, or assisting in the conduct of a particular research study or trial. Such information collected will include name, address, contact details, professional qualifications and

experience, and registration information.

We may collate statistical data from study/trial results that we have collected over years for the purposes of future research, or advising on healthcare policy to Governments and decision-makers.

- ***General Activities***

  As part of the ordinary course of business operations, we will capture and record personal information from our dealings with partners, business alliances and service providers. Such information is collected for administrative, management, and audit purposes.

  We may collect personal information (e.g. name and contact details) from those who contact us (by phone or in person). Also, when accessing our websites (refer to 'How do we collect and hold your personal information' section below). Such information is collected in order to deal with you and improve our services.

  We are required to collect personal information from donors and supporters of TGI in order to comply with laws and issue tax receipts. Information collected will include name, contact details and payment details. We may collect personal information when we are canvassing recruitment of staff and PhD students. You may also supply personal information to us when applying for open positions, and we may collect your personal information from third-parties (e.g. referees) as part of the assessment and recruitment process. Such information collected will include educational and academic background, work history, skill-set and capabilities. We will collect similar personal information from volunteers who apply to work with The George Institute.

Can you deal with us anonymously?

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 The George Institute undertakes).

How do we collect and hold your personal information?

- ***Research Studies***

  We aim to collect your personal information directly from you:

  - when you first make contact with us (e.g. phone, in person, email or via our website);
  - when you agree to participate in a research study or trial (e.g. through the study information/consent process); and
  - when dealing with us as part of ordinary business.

  We may collect your personal information from a third-party, such as your medical or health provider (e.g. GP, hospital) and an information document (including requisite privacy disclosures) will be given to you by that provider.

- ***Our Websites***

  When accessing our websites, we may make a record of your user service address and internet provider name and address, the date and time of your visit, the pages you accessed and any documents downloaded, any website visited prior to accessing our site and the type of browser used. This information (which is unlikely to contain personal information) is collected to monitor the activity on our websites (including the popularity of certain pages and information presented on our websites, and linkages to information), to consider improvements to the delivery, presentation and types of information our websites (including cost/benefit analysis), and ensure the protection of our

intellectual property and reputation.

Our websites do use cookies, which are small text files that are stored your local browser cache when you visit a website. Using cookies makes it possible to recognise the visitor's browser in order to optimise the particular website and simplify its use. Information collected via cookies is not used by us to determine the personal identity of a visitor. Most browsers are set up to accept these cookies automatically. You can deactivate the storing of cookies or adjust your browser to inform you before a cookie is stored on your computer.

- ***Holding personal information***

We hold personal information in paper-based and electronic records and systems.

Personal information collected in paper-based documents may be converted to electronic form for storage (with the original paper-based documents either archived or securely destroyed).

The George Institute uses physical security and other measures to ensure that personal information is protected from misuse, interference and loss, and from unauthorised access, modification and disclosure.

Personal information held in paper-based form is generally securely stored at our offices, with archived records held at an external storage facility. Our databases and their contents remain at The George Institute and stay with data processors or servers acting on our behalf and responsible to us.

We maintain computer and network security by using firewalls, user identifiers and passwords to control access to our computer system.

Donations and registrations made on The George Institute website use encryption methods and credit card data is stored using systems compliant with the Payment Card Industry Data Security Standard.

How do we disclose your personal information?

- ***Research Studies***

We may disclose your personal information to our staff, related parties, and approved third-parties (e.g. agents, service providers, collaborators and research partners) who are working on the study or research program for which your personal information was collected; but only to such persons who need to know. Our staff must comply with privacy and confidentiality terms as part of their employment with us. To be an approved third-party of TGI, that party must be subject to similar privacy and confidentiality laws, or have a professional and/or contractual obligation of confidence.

We may also disclose your personal information as directed or permitted by law or court order.

Depending on the circumstances and the location where the study or research program is being conducted or coordinated, the above-mentioned may involve a cross-border disclosure. Our studies are often internationally based and our staff, agents, service providers, collaborators and research partners may be located overseas, e.g. Canada, the United Kingdom, the European Union, India and China. This will be explained in the study protocol and information documents.

Whenever possible, your personal information will be de-identified (and aggregated with others) before disclosure.

- ***General Activities***

It is unlikely that personal information collected outside a study or research program (such as information collected during the ordinary course of business activities) will be disclosed outside of The George Institute.

Data Security

We have put in place measures to protect the security of your information, and to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access (by physical and technical safeguards) to your personal information to those staff, related parties, and approved third-parties (e.g. agents, service providers, collaborators and research partners) who have a business or legal need to know.

We have also put in place procedures to deal with any suspected data breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Marketing

We may use your personal information to offer you products and services which we believe may interest you, but we will not do so if you tell us not to.

Where you receive electronic marketing communications such as event communications and newsletters from us, you may opt out of receiving further marketing communications by following the opt-out instructions provided in the communication.

For individuals located in the EEA

- ***Your rights***

  If you are located in the European Economic Area (collectively the EEA) you will have certain rights under the GDPR:

Rights	What does this mean?
The right of **access**	You have the right to obtain access to your personal information that we hold about you.
The right of **rectification**	You are entitled to have the personal information that we hold about you corrected if it is inaccurate or incomplete.
The right to **erasure**	This is also known as “the right to be forgotten” and enables you to request the deletion or removal of your personal information if there is no compelling or legal reason for us to keep using it.
The right to **restriction of processing**	You have the right to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
The right to **object to processing**	You have the right to object and ask us to stop processing your personal information.
The right to **lodge a complaint**	You have the right to lodge a complaint about the way we process your personal information with a supervisory authority in the EEA.

The right to **request transfer**	You have the right to request us to transfer personal information we hold about you to another party, in a machine readable format.
The right to **withdraw your consent**	You have the right to withdraw your consent to us processing your personal information.

These rights are not absolute and may not apply in all circumstances.

➢ ***Legal basis for processing***

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where you have given consent;
- Where we need to perform the contract, we have entered into with you;
- Where we need to comply with a legal obligation; or
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

Please contact us should you require any additional information about the legal grounds we rely on for any specific processing activities that involve your personal information.

➢ ***How long will we keep your information?***

We will only retain your personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

How can you access and seek correct of your personal information held by us, or exercise other rights under GDPR?

You may request access to, or seek correction of, your personal information that is held by The George Institute, or exercise other rights available to you under GDPR, by writing to the Privacy Officer:

- Address: Level 5, 1 King Street Newtown; or
- Email: privacy@georgeinstitute.org

We will generally not charge a fee for such requests, but we may charge a reasonable fee if your request is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Typically, we will respond to your request within 10 - 20 business days but sometimes we may require more time depending on the circumstances.

In your request, please ensure that you provide a reply address, so that we can contact you if we are unable to locate your personal information, if we need to verify your identify, or if we cannot carry out your request (in which case, we generally tell you why).

What should you do if you have a complaint about the handling of your personal information?

Please set out your complaint in writing to the Privacy Officer:

- Address: Level 5, 1 King Street Newtown; or
- Email: privacy@georgeinstitute.org

Please provide sufficient information, so that the Privacy Officer can consider your concerns and contact you. Typically, we will respond to your complaint within 10 - 20 business days.

If you are not satisfied with our response, or you consider that we may have breached the Australian Privacy Principles or the *Privacy Act 1988* (Cth), you are entitled to make a complaint to the Office of the Australian Information Commissioner. The Office of the Australia Privacy Commissioner can be contacted by telephone on 1300 363 992 or full contact details can be found online at www.oaic.gov.au.

If you are located in the EEA you may wish to lodge a complaint with a supervisory authority within the EEA. Please click here for a list of the national data protection authorities in the EEA.

How are changes to this privacy policy made?

We may amend this Privacy Policy from time to time, with or without notice to you.

Please refer to our corporate website www.georgeinstitute.org for the latest copy.