Due to the unique nature of the services we provide, GP partners Australia ™ (GPpA) handles large volumes of written and electronic information on a daily basis. This information originates from a wide range of sources, and includes:

1. Internal information that pertains to the day to day running of the GPpA, such as employee records, financial records and records of inquiries or services provided to General Practices, Government bodies, or any other interested stakeholders.

2. Statistical (de-identified) patient data received from General Practices through the GPpA's Data Extraction Tools.

3. General health information relevant to the area in which the GPpA operates.

4. Information about General Practices and any other interested stakeholders, such as contact names, qualifications, contact details, specializations or details of services provided.

5. Identified patient referral information for the mental health service and the national diabetes care pilot.

Given the importance of confidentiality in health or any health related services, GPpA and its employees must ensure that all information, regardless of the type of information, is treated in a manner that respects the privacy of any person to whom information relates, and complies with Australian Privacy Principles (2014) where appropriate.

BEST PRACTICE

The following principles apply to all written or electronic information collected by the GPpA that is not in the public domain, regardless of the information's origin or nature, and whether it identifies a particular person or not):

1. Information will only be collected if it is necessary for the GPpA's operational activities and to provide its services or improve its services to General Practices and/or the general population.

2. Access to either hard copy or electronic information should only be granted to those employees who need to access information due to their role within the GPpA.

3. The GPpA will maintain a reasonably secure environment for all information that it collects uses or discloses and will take reasonable steps to prevent any information being lost, misused, altered or inadvertently destroyed.

4. If an employee of GPpA, any General Practice or any other appropriate stakeholder has a legitimate reason for wanting to access information held by GPpA, then GPpA will review each request carefully and determine whether the request access (and the reasons) is appropriate in the circumstances.

5. GPpA must ensure that the information it handles is as accurate and as up to date as possible.

6. GPpA will ensure that all staff executes confidentiality deeds or agreements to ensure each person's commitment to these principles, and the confidentiality of information.

7.

THE PRIVACY ACT

The Privacy Act 1988 (**"Act**") regulates the way the GPpA handles particular types of information. The GPpA Privacy Rules (**"GPpA PRs**") that form part of this Policy details the procedures that the GPpA has in place, in addition to the best practice requirements defined above, to ensure compliance with the Act.

THE GPpA PR

The GPpA PR's regulate the handling of personal information for the development or improvement of, or provision of, GPpA's programs and services. Importantly, the GPpA PRs only apply to personal information.

Personal Information identifies a particular person by name, or contains enough detail for someone to identify who the person is, and does not necessarily have to be true (and could merely be an opinion). Examples include:

- Any health information that has a name or identifier attached.
- Personal details, such as a name, address, consultation dates, billing information, health insurer information and Medicare number.
- Information generated by a medical practitioner or clinician such as notes and opinions about an individual and their health.
- Information about medical samples, such as test undertaken by a laboratory, where an individual can be identified.

Personal Information is not:

- Records relating to employees of GPpA.
- De-identified information and statistical data sets obtained by the GPpA through its Data Extraction Tools that do not allow the identification individuals.
- Information that is publicly available, such as publications, leaflets or like information obtained from the internet.
- Information about deceased persons or a corporate entity, such as the name, address or other information relating to companies.

The Act places special emphasis on the health information referred to above and is specifically defined to include any personal information collected by a health service provider during the course of providing treatment and care to an individual. This will apply to all General Practices but will ordinarily not be the case for GPpA, who obtains aggregated data.

DATA EXTRACTION TOOLS

Of particular concern for the GPpA is information obtained from General Practices through its Data Extraction Tools, such as the Practice Health Atlas, the NPI Data Extraction Tool and the PCS Clinical Audit System ("Statistical Data.") Ordinarily the Statistical Data obtained by the GPpA is de-identified and will not be covered by the GPpA PR.

If health information is unable to be identified with the particular individual, it is no longer 'personal health information' any privacy concerns are minimal. With consent from the owner (i.e. General Practice) of the source of such data, statistical Data can then be disclosed to third parties and for a range of specific purposes, but always subject to the Best Practice Directions referred to in this Policy.

De-identification of personal health information requires more than removing a patient's name. To ensure that the Act is not breached, the Data Extraction Tools will be applied to ensure the following:

1. Data obtained by the GPpA must be aggregated to the postcode level, which is many times larger than an individual collection district.

2. Data used by the GPpA must be coded on a range of scales when mapping. For example, the distribution may be presented as percentiles (1%–5%, 5%-10% and so on). Postcodes are not displayed, so that it would not show a postcode with less than 5 persons. With this approach to aggregation of data it would be very difficult to identify any individual patient.

3. The use of patient identification numbers instead of names must be used. However, patient identification numbers must not be derived from the patient's name, date of birth, address, telephone number, Medicare number (or any other identifier assigned by a Commonwealth agency) or any other information that could identify the person.

If for whatever reason any Statistical Data that identifies an individual (or has the capacity to identify an individual) comes into the possession of the GPpA, the GPpA PR must be immediately applied.

PRIVACY OBLIGATIONS ON GENERAL PRACTICES

When a staff member of the GPpA provides support for a practice, be it with an individual General Practitioner, Practice Nurse or other Practice staff member, it is clearly understood that any patient data is data owned by the practice.

It is the responsibility of each General Practice to ensure they have a comprehensive Privacy Policy in place. Unlike the GPpA (where patient information and data sets are aggregated and de-identified by the time the information is obtained by the GPpA) information at each General Practice will contain identifiers and will be considered Health Information.

GPpA takes no responsibility for the suitability or otherwise of the policies in place at each General Practice it services, but would expect at a minimum that a policy is in place that sets out who is responsible for overseeing the implementation and effective operation of the privacy policy, and a single point of contact for privacy issues.

As a matter of best practice, each General Practice should inform their patients of the possible uses of the Statistical Data, and should ensure that no patients have any objections to its use in this manner.

With regard to the individual patient, the process of consent relating to the individual patient rests with the patient and the General Practice. When the patient provides any information or data to the practice, there should be a clear explicit understanding between the patient and the GP, that the GP and his/her support team will use the data for ongoing quality improvement in clinical assessment, practice systems and service delivery, and care of the patient. Most practices have a consent process established as part of their accreditation process.

Any process of data collection from practices will therefore require a written consent process that clearly articulates the Practice's responsibility to have in place a policy dealing with its approach to privacy and data management.

THE GPpA PR AND A PRIVACY OFFICER

A Privacy Officer will be appointed by GPpA who will be responsible for ensuring this Policy remains up to date, accurate, and as far as is reasonably possible, is complied with by the GPpA and its employees.

The Privacy Officer is Helen Shaw who will be responsible for responding to any requests for information or access to information. The Privacy Officer will also be responsible for advising any individual who lodges a complaint with the GPpA alleging a breach of the Act or the GPpA PR that, if the GPpA does not satisfactorily address their grievance, that they can contact the Federal Privacy Commissioner on 1300 363 992.

GPpA PRIVACY RULES[1]

Principle	Description
APP 1 **Open and transparent management of personal information** An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.	1.1 This policy will be made available to any person requesting access to it. A general statement, such as a brochure describing our approach to privacy will be on public display at the GPpA.
APP2 **Anonymity and pseudonymity** Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do so.	2.1 Where it is lawful and practicable to do so, the GPpA will allow individuals to provide information anonymously. 2.2 The GPpA will have a privacy alert system in place, to ensure that a privacy request is recorded and respected. 2.3 An individual who chooses to access the services of the GPpA anonymously will be advised of any potential consequences resulting from their decision, for example where the lack of a contact name or address may jeopardise care in an emergency situation. 2.4 The GPpA will not automatically preclude an individual from participating in the activities of the GPpA because they request anonymity, but the GPpA may insist upon the provision of the information if it has concerns that the anonymity could create a health risk of some description.
APP3 **Collection of solicited personal information** An organisation must not collect sensitive information unless the individual has consented, it is required by law, or in other	3.1 The GPpA will only collect sensitive information (as defined under the Act) including health information about an individual if: 3.2 the individual provides their written consent to the GPpA or the Practice from which the information is obtained;

[1] The GPpA PR is based on the Australian Privacy Principles (APP) in Schedule 3 of the Act. The phrase 'personal information' is as defined in this Policy.

Principle	Description
special specified circumstances, for example, relating to health services provision and individual or public health or safety.	3.3 the collection is required by law; or 3.4 such collection is consistent with the provisions of APP 10
APP4 **Dealing with unsolicited personal information** Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, how it may be used or disclosed, and be advised that the person can get access to their personal information and also be advised what happens if the person decides to withhold any information from the GPpA	4.1 The GPpA will only collect personal information that it needs to provide its services to General Practices (including obtaining or providing Statistical Data) to undertake our programs, activities and functions, and to provide general management functions. 4.2 Personal information about any person (including Practice patients or people the GPpA deals with directly) will only be collected in a lawful manner and will be obtained directly from the individual after obtaining their permission to do so. 4.3 If a person refuses to provide personal information, the risks of not doing so (such as not being able to contact them if necessary) will be explained. 4.4 The name and telephone number of the Privacy Officer will be provided to any person who provides personal information to the GPpA. 4.5 The GPpA will ensure that any person who provides personal information is told why the GPpA needs to collect the information and how the information will be used. This includes how and if their personal information may be given to a third party. Any explanation will make clear that the nature of the services provided by the GPpA make the provision of the information necessary, and that the information is required for the GPpA to carry out its role effectively. 4.6 The GPpA must make sure that individuals providing personal information understand the consequences, if any, of providing

Principle	Description
	incomplete or inaccurate information.
APP5 **Notification of the collection of personal information**	5.1 At the commencement of an individual's dealings with the GPpA, an individual will be given the opportunity to indicate if they wish to refuse consent to the release of their personal information to any specific person(s) or entities and the effect this may have on service provision. They will be given a form (Release of Information Form) where they can record this. 5.2 If the individual does not complete this form after being provided with same (and does not verbally refuse) the GPpA is able to assume that the individual agrees to the release of their personal information.
APP6 **Use or disclosure of personal information** An organisation should only use or disclose information for the primary purpose it was collected, unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.	6.1 This GPpA will ensure that personal information is only used for the main reason it was collected, or for a secondary reason that would reasonably be expected by the individual providing the information. Ordinarily, personal information will be obtained to assist and further the GPpA's main goals of providing its services to General Practices and any other interested stakeholders. Individuals will be told that the information may be provided to our interested stakeholders (such as General Practices, individuals or government departments) but only with the consent of the individual concerned. Ordinarily it would be expected that any personal information will be de-identified prior to transmission. 6.2 If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, the GPpA will obtain informed consent from the individual, or will ensure that the Practice who provides the information obtained the consent of the individual. 6.3 Individuals will be given the opportunity to refuse such use or disclosure.

Principle	Description
	6.4 If an individual is physically or legally incapable of providing consent, a responsible person (as described under the Act) may do so. 6.5 We will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the individual's or the public's health and safety. 6.6 We will keep records of any such use and disclosure. 6.7 Information may be disclosed to a responsible person (as described under the Act).
APP7 **Direct marketing**	7.1 GPpA will only use or disclose personal information for direct marketing purposes if an exception, listed in APPs 7.2 to 7.5, applies
APP8 **Cross border disclosure of personal information** An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.	8.1 The GPpA will only transfer personal information interstate or overseas about an individual to someone who is in a foreign country if: 8.2 the individual consents to the transfer and directs the GPpA to do so; or 8.3 the recipient is bound by legislation that is substantially similar to the APPs; or 8.4 The GPpA is reasonably sure that the information will not be held, used or disclosed inconsistently with the APPs.
APP 9 **Adoption, use and disclosure of government related identifiers** Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government 'agency'.	9.1 Except where circumstances allow (APP9.1), the GPpA will not use any identifiers of this nature, such as Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State/Territory agency to identify personal information.
APP10 **Quality of personal information**	10.1 The GPpA will take reasonable steps to ensure that personal information kept, used or disclosed by the GPpA is accurate, complete, and as up to date

Principle	Description
An organisation must take reasonable steps to make sure that the personal information it collects uses or discloses is accurate, complete and up-to-date	as practicable. 10.2 This will include, on a regular basis, querying with individuals whether their personal details have changed. 10.3 Any brochures or forms setting out Privacy obligations must contain a clause that requires the individual to notify the GPpA immediately should any information they have provided be changed.
APP11 **Security of personal information** An organisation must take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.	11.1 All personal information held by the GPpA will be: accessible by staff only on a "need to know" basis; 11.2 not removed from the GPpA offices unless authorised and for a specified purpose. 11.3 If the information is electronic and stored on a laptop or like device, this will be password protected and not sent via email or uploaded to the internet for any reason. The file or identifying data can only be transferred by physical medium (such as a hard drive or USB key.) 11.4 If the information is in hard copy, it will be stored in a manner that is only accessible by authorised staff and can not readily be accessed by an unauthorised person. 11.5 Access to the GPpA's records and computer systems is controlled and closely monitored. Staff and authorised external users have restricted access only to the systems that their duties require and will have executed appropriate confidentiality deeds or agreements. 11.6 The computer systems have security passwords and all staff are bound by a strict code of conduct. 11.7 The GPpA will destroy or permanently de-identify personal information that is no longer required by the GPpA.

Principle	Description
APP12 **Access to personal information** Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.	12.1 Under normal circumstances the GPpA will provide an individual access to their personal information within 30 days of receiving a request for access. 12.2 There will be no fee associated with lodging a request for access, however, a small but reasonable administration fee may be charged. 12.3 Provision of access to a person's personal information will be undertaken in a way that is appropriate to the person's particular circumstances, for example the use of interpreters. 12.4 If an individual believes that information held by the GPpA is inaccurate or incomplete, the GPpA will take steps to amend or correct the information. 12.5 The GPpA may refuse access if it reasonably believes that: 12.6 A person's health, safety or wellbeing may be compromised by releasing the information; or 12.7 Providing access would be unlawful or would prejudice a legal investigation. 12.8 Under circumstances other than 6.4.1 and 6.4.2 where information is withheld, the GPpA will ensure that its practices are consistent with the provisions of NPP 6. 12.9 If information is withheld under 6.4, the GPpA will provide an explanation to the individual as to the reasons why this was the case.
APP13 **Correction of personal information**	13.1 GPpA shall take such steps (if any) as are reasonable in the circumstances to correct information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading

Page 11 of 11