1.1 **Privacy Policy**

In compliance with the *Privacy Amendment (Private Sector) Act 2000*, this practice has prepared this privacy policy to describe the way and circumstances under which personal information is collected, stored, used, and disclosed and also how complaints are handled by this practice.

1.1.1 Privacy Statement

AUSTRALIAN PRIVACY PRINCIPLES (APP) POLICY

PART A – PURPOSE AND CONTEXT

1.0 Thrive Medical is committed to ensuring the privacy and confidentiality of all personal information affiliated with Thrive Medical's business undertakings.

1.1 Thrive Medical follows the terms and conditions of privacy and confidentiality in accordance to the Australian Privacy Principles (APPs) as per schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), forming part of the Privacy Act 1988 ('the Act').

1.2 The purpose of this Privacy Policy is to clearly communicate how Thrive Medical collects and manages personal information.

1.3 The point of contact regarding any queries regarding this policy is the Practice Manager, (07) 4019 2960.

PART B – AUSTRALIAN PRIVACY PRINCIPLES

2.0 As a private sector health service provider and under permitted health situations, Thrive Medical is required to comply with the APPs as prescribed under the Act.

2.1 The APPs regulate how Thrive Medical may collect, use, disclose and store personal information and how individuals, including Thrive Medical's patients may:

- address breaches of the APPs by Thrive Medical;
- access their own personal information; and,
- correct their own personal information.

2.2 In order to provide patients with adequate health care services, Thrive Medical will need to collect and use personal information. It is important to be aware that if the patient provides incomplete or inaccurate information or the patient withholds personal health information Thrive Medical may not be able to provide said patient with the services they are requesting.

2.3 In this Privacy Policy, common terms and definitions include:

- "Personal information" as defined by the Privacy Act 1988 (Cth). Meaning "information or an opinion including information or an opinion forming part of a database, whether true or not, and whether recorded in a material format or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion"; and,
- "Health information" as defined by the Privacy Act 1988 (Cth). This is a particular subset of "personal information" and means information or an opinion about:
  - the health or a disability (at any time) of an individual;
  - an individual's expressed wishes about the future provision of health services to them; or,
  - a health service provided or to be provided to an individual.

2.3.1 Personal information also includes 'sensitive information' which is information including, but not limited to a patient's:

- race;
- religion;

- political opinions;
- sexual preferences; and or,
- health information,
- preferred pronouns

2.3.2 Information deemed 'sensitive information' attracts a higher privacy standard under the Act and is subject to additional mechanisms for the patient's protection.

PART C – TYPES OF PERSONAL INFORMATION

3.0 Thrive Medical collects information from each individual patient that is necessary to provide said patient with adequate health care services.

3.1 This may include collecting information about a patient's health history, family history, ethnic background, or current lifestyle to assist the health care team in diagnosing and treating a patient's condition.

PART D – COLLECTION & RETENTION

4.0 **APP 5 – Notification of the Collection of 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, that the person can get access to their personal information and what happens if the person does not give the information.

Policy

This practice will only collect personal information necessary to provide our patients with a quality health service. information about a patient will only be collected by lawful and fair means and directly from the patient wherever possible.

Wherever practical this practice will only collect information directly from the patient via treatment forms, medical consult forms, face to face consultations etc. This may not be possible if the patient is unconscious or otherwise incapable of providing that information. If information is collected about a patient from another party, this practice, will whenever possible, advise the patient of this.

In other instances, Thrive Medical may need to collect personal information about a patient from a third-party source. This may include:

- relatives; or,
- other health service providersallied health providers;
- electronic transfer of prescriptions (e-scripts)
- My Health Record eg. Via shared health summary, event summary
- Government medical services eg Q-script, The Viewer, HPOS and PRODA

We will ensure that each patient providing personal information is informed about and understands the. purpose of collecting the information. They will also be advised as to whom or under what circumstances their personal information may be disclosed to another party and how they can access the information held about them by this practice. This will be carried out via the Thrive Patient Privacy Policy and/or brochures and/or verbally.

We will ensure that patients who are asked to provide personal information understand the consequences, if any, of providing incomplete or inaccurate information.

This will only be conducted if the patient has provided consent for Thrive Medical to collect the information from a third-party source; or, where it is not reasonable or practical for Thrive Medical to collect this information directly from said patient. This may include where:

- the patient's health is potentially at risk and their personal information is needed to provide them with emergency medical treatment.

4.1 **APP 2 – Anonymity and Pseudonymity**

Organisations must give people the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

Does not apply if:

a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Policy

This practice has deemed it impracticable to treat a patient on an anonymous basis primarily due to safety concerns for our clinicians. Other reasons for supporting this decision include not being able to keep accurate records, follow up with reports, provide medical reports and ensure reliable payment.

If a new patient cannot provide reception team members with a form of identification upon arrival, they will be informed of the following:
- The consultation will need to be paid privately, there will be no Medicare rebate.
- No scripts can be given.

1.2 **APP 4 – Dealing with Unsolicited Personal Information**

If you receive personal information and you did not solicit the information, you must, within a reasonable period after receiving the information, determine whether you would have been permitted to collect the information under Australian Privacy Principle 3 (collection).

Policy

- If unsolicited information has been received the treating GP must determine whether our practice would have been permitted to collect the information under APP3 (collection).
- If the information could not have been collected under APP3, reception team members will contact the sender to arrange the return of information. If this is not possible or practicable the information is to be destroyed.
- If it is the type of information that our practice could have been permitted to legally collect then we are able to deal with the information as we would any other according to APPs 1-5.

1.3 **APP 5 – Collection of Solicited Personal Information**

An organisation must not collect personal information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety.

Policy

This practice will only collect sensitive information other than health information about a patient if:

the patient consents; or
the collection is required by law

1.4 **APP 9 – Adoption, Use or Disclosure of Government Related Identifiers**

You must not adopt a government-related identifier of an individual as your own identifier of the individual unless the adoption of the government-related identifier is required or authorised by or under an Australian law or a court/tribunal order.

You must not use or disclose a government-related identifier of an individual unless the use or disclosure of the identifier is reasonably necessary to verify the identity of the individual for the purposes of your activities or functions; or
• the use or disclosure of the identifier is reasonably necessary to fulfil your obligations to an agency or a State or Territory authority; or
• the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order.

Policy

- Medicare cards & Veterans Affairs numbers will not be used to identify the patient in our practice.

1.5 **APP 10 – Quality of Personal Information**

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.

Policy

This practice will take reasonable steps to ensure that personal information kept, used, or disclosed by the practice is accurate, complete, and as up to date as practicable.

Medical records are confidential legal documents. Doctors and team members have a responsibility to maintain the privacy of every medical record, which is each patient's right. As a key component for the continuing management of our patients, accurate and complete records are kept.

Each patient has an individual medical record incorporating a health summary, progress notes, referrals made, and responses received including pathology, x-ray; documentation of telephone calls, home visits, after hours communication and all hospital visits made.

Doctors, practice nurses, allied health practitioners and authorised students of this practice are responsible for documenting their own notations for care given to their patients. For each consultation the doctor notes the following details in the medical record:

Doctor's name
Date
Reason for consultation
Other problems managed
Management plan
Planned dates for review
Medications prescribed with route, frequency, other directions for use and number of repeats
Preventative care
Referrals to other health care practitioners
Consent issues

Appropriately filed pathology, x-ray and related referrals and results are in the medical record.

All entries are dated and initialled or signed. Information in the medical record is not prejudicial, derogatory nor irrelevant and is legible being able to be read by other health care practitioners for the ongoing management of the patient.

Referrals to other health care providers contain sufficient information for continuing health management with signature, designation, and date. A copy remains in the medical record.

Patients who attend our practice on a regular basis have a health summary included in their medical record. The record also contains family and social history, past and active problems, allergies and sensitivities, medication, immunisation status and any risk factors present.

Reception regularly ask patients upon arrival if their personal details need to be updated.

PART E – PURPOSE OF COLLECTION, USE & DISCLOSURE

5.0 APP 6 - Use or Disclosure of Personal Information

An organisation should only use or disclose information for the 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.

Policy

This practice will ensure that personal information will only be used for the purpose it was collected, or that would reasonably be expected by the patient providing the information. If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, we will obtain informed consent from the patient.

- Individuals will be given the opportunity to refuse such use or disclosure.
- If a patient is physically or legally incapable of providing consent, a responsible person (as described under the Act) may do so.

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 patient's or the public's health and safety.

- We will keep records of any such use and disclosure.

Information may be disclosed to a responsible person (as described under the Act).

5.0.1 Notifiable Diseases

Policy

Under Infectious Diseases Act - Health (Infectious Diseases) Regulations in Sections 146, 390 and 391 of the Health Act 1958, medical practitioners are to report infectious diseases as specified. Notifications of cases are made to the Central Public Health Unit.

Procedure

It is the responsibility of the treating doctor or nominated person to notify the Tropical Public Health Unit of any communicable diseases.

5.0.2 Medical Students

Policy

Patients may not wish to have their personal health information used for education purposes. This practice respects its patient's right to privacy and where possible will use de-identified data for case studies. We will always inform patients of impending medical students participating in practice activities and ask patients to consent to this.

5.0.3 Research and Quality Program

Policy

Where it is desired to publish material related to clinical work or for practice continuous quality improvement activities, the anonymity of patients is to be preserved. Research requests are to be approved by the practice principal.

The patient must consent to any specific data collection for research purposes. If the data is required by or in accordance with rules established for accreditation by RACGP or other diligent professional health agencies, then data will be de-identified where possible, with related obligations of confidentiality upon health professionals engaging in these activities.

Procedure
All patients are asked on registration if they consent to having their medical record reviewed as part of quality improvement (QI) activities at this practice. This is formatted as a yes or no box to tick on the "New Patient Information" form and they are required to sign at the bottom of the form. When an existing patient, who has not previously consented to their data being utilised for QI activities, books for an appointment, they are provided with a consent form to complete. This form is scanned to their medical record. An annotation is made in the patient's appointment notes 'Consents to QI' or 'Does not consent to QI'.

5.0.4 Disease Registers (For Public Health Purposes)

Policy

For cervical screening, breast screen and other disease specific registers consent is required from the patient to use their personal health information for this purpose. The patient is given the opportunity to decline inclusion in these types of registers.

5.0.5 My Health Record

Policy
Organisational team members must only access the My Health Record system if this access is required by the duties of their role.

The following roles are responsible for implementation and compliance monitoring of My Health Record policy in our practice:

- Our RO, (Practice Manager) oversees our practice's legal compliance and sets up procedures to facilitate compliance with My Health Record legislation.
- Our OMO, (Practice Manager), is responsible for implementation and compliance monitoring of My Health Record policy, and for maintenance of the policy within our practice.

Individuals wishing to access My Health Record must have a registered Health Provider Identifier (HPI-I) number. Specific training on how to access My Health Record must be completed during commencement of employment and is a responsibility of the practice manager. Organisational team members must only access the My Health Record system if this access is required by the duties of their role.

In our practice we collect and record the Healthcare Provider Identifiers (HPI-Is) of our healthcare providers at the beginning of their employment. This number is verified once inputted into the team members Best Practice profile. The list of health providers is kept up to date by the practice manager.

5.0.5.1 Assisted registration:

Our practice does provide assisted registration for patients. Cairns is an area where an MHR was automatically created for everyone unless they opted out. Assisted registration may be required for patients who initially opted-out from having a record created but who now want a record.

Procedure:
1) Obtain consent from patient.
2) Verify their identity with Medicare card and driver's licence.
3) Follow the steps through Best Practice to register.

5.0.5.2 Requests to access a patient's My Health Record:

Our practice has established processes for identifying a person who requests access to a patient's My Health Record.

5.0.6 Subpoena, Court Order, Search Warrant and Coroner

Policy

Information will be released if a subpoena, court order, search warrant or coroner is received. If the doctor is concerned about confidentiality issues, they may decide to challenge it in court if sufficient evidence amounts to possible breach in confidentiality.

Procedure

1. Inform the patient's doctor via messaging system and import the request into the doctor's inbox.
2. Record the date of court case in the patient's medical record.
3. Once the doctor has reviewed the patients file and given approval make a copy of the record.
4. Retain the copy in file and mark as a duplicate on each page with reason for the copy noted inside.
5. Sometimes a team member is required to take the medical record to court. Telephone the relevant solicitor or Clerk of courts and try to arrange a confidential courier to transport the record in, as an alternative.
6. Telephone closer to the day requested, if a team member must take the record physically to court, to ensure the date is correct and the case is still on.
7. Return the record to the practice after the review by the court unless otherwise instructed by the court.

5.0.7 Relatives and Friends

Policy

No information is to be released unless the patient has authorised that person to act on their behalf or access has been given through a signed legal authority.

Separate records are advised for all family members but especially for children whose parents have separated, and care must be taken that sensitive demographic information about either partner is not recorded on the demographic component of the record.

Our practice believes that from the age of 15, patients becoming solely responsible for their healthcare unless they authorise another person (parent, caregiver ect) toact on their behalf. Patient between the age of 15 and 18 are required to give written consent for information to be provided to persons other than themselves (see section 10 - 15 Years and Over Patient Consent Form).

5.0.8 Police and Lawyers

Policy

Police and lawyers must obtain a .o0signed patient consent (or subpoena, court order or search warrant) for release of information. The request is directed to the doctor. Where only a signed patient request is obtained the doctor is not legally obliged to release information.

5.0.9 Insurance Company and Social Welfare Agency

Policy

No information to be given without express written consent from the patient. All enquires must be directed to the patient's doctor. Release of information is an issue between the patient and the doctor.

5.0.10 Employers

Policy

If the patient has signed consent to release information for a pre-employment questionnaire or similar report then direct the request to the doctor who will respond with the required information. Otherwise, no information is to be released. When in doubt always refer the request to the doctor. Patient may seek access via privacy law.

5.0.11 Emergencies

Policy

Where immediate treatment is necessary to preserve a life or prevent serious injury, all attempts are made to gain the patient's consent. This may not be successful in all cases prior to administering emergency care.

5.1 Informed Consent

Policy

Our doctors inform their patients of the purpose, benefit and risks of proposed treatment or investigations. We believe that patients need to receive sufficient information to allow them to make informed decisions about their care.

Information is clear and given in a form that is easy to understand, whether it be verbally, in a diagram with explanation, brochure, other handout/leaflet or poster eg. available in our waiting room.

Doctors take into consideration the patient's ethnicity and principal language spoken. Steps are taken to ensure an interpreter is utilised where necessary and at the patient's request. Issues of personality, personal fears and expectations, beliefs and values are also considered.

There is no coercion by our doctors. Our patients can choose to reject their doctor's advice or seek a second opinion. Doctors also inform patients of potential additional costs and out of pocket expenses for treatments and investigations, prior to them being carried out, whether they would be done on site or referred to medical specialists.

Patients are asked to be open and should be able to feel free to discuss all health issues and proposed treatments, without the fear of reprisals.

Patient consent is obtained for the following:

Operative procedures on-site (written consent)
Patient's personal health information sought for research projects (written consent)
Clinical training program (verbal consent)
Third party observation or participation in patient consultation (verbal consent)

The Privacy Act states that consent may be 'express' or 'implied'.

Express Consent – clear and unmistakably states, obtained in writing, orally or in any clear other form where consent is clearly communicated.

Implied Consent – patient presents to doctor, discloses health information and this is written down by the doctor/entered on computer during the consultation, e.g., doctor collects specimen and sends it to pathology, reason to consider that the patient is giving implied consent to passing necessary information to the laboratory.

5.1.1 Consent Forms

Policy

Consent forms for treatment are available as templates in the Best Practice software and are to be used by the doctor for patient consent to on-site procedures. The doctor explains the form to the patient and completes it with the patient signature.

Procedure

Doctors inform patients of the following issues concerning treatment and investigations:

Possible nature of illness/disease.
Proposed approach to investigation, diagnosis and treatment including describing if it is conventional or experimental, common side effects and the clinician undertaking the procedure/treatment.
Purpose, importance, benefits, and risks.
Other options.
Length of procedure/treatment.
Approximate indication of costs involved including out of pocket expenses.
Degree of uncertainty of a) any diagnosis found and b) therapeutic outcome.
Potential result of not undertaking the specified procedure/treatment or any other treatments

5.2 Direct Marketing

APP 7 -DIRECT MARKETING

If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Policy

- This practice will not use personal information obtained to send direct marketing material to a patient unless consent is given.
- The individual will also be given a chance to opt-out when the material is sent.
- Sensitive information will not be used for direct marketing purposes.

5.3 Government Related Identifiers

APP 9 – Adoption, Use or Disclosure of Government Related Identifiers

You must not adopt a government-related identifier of an individual as your own identifier of the individual unless the adoption of the government-related identifier is required or authorised by or under an Australian law or a court/tribunal order.

You must not use or disclose a government-related identifier of an individual unless the use or disclosure of the identifier is reasonably necessary to verify the identity of the individual for the purposes of your activities or functions; or
• the use or disclosure of the identifier is reasonably necessary to fulfil your obligations to an agency or a State or Territory authority; or
• the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order.

Policy

- Medicare cards & Veterans Affairs numbers will not be used to identify the patient in our practice.

PART F – ACCESS AND CHANGES TO PERSONAL INFORMATION

1.0 Access to Personal Information

APP 12 – Access to Personal Information

If you hold personal information about an individual, you must, on request give the individual access to that information.

Policy

If an individual patient reasonably requests access to their personal information for the purposes of changing said information they must engage with the relevant practice manager.

Under normal circumstances this practice will provide a patient with access to their personal information within 30 days of receiving a request for access.

All requests are to be provided in writing through use of the Request for Access form (see section 10 - Request to Access Medical Records Form). Identification is also requested to ensure that a false application is not lodged.

There will be no fee associated with lodging a request for access, however, an administration fee may be charged as set out in the Request for Access application.

Patients will be provided with an opportunity to discuss their personal information with an appropriate member of team members when access is sought, however a fee for the doctor's time may be charged.

Provision of access to a patient's personal information will be undertaken in a way that is appropriate to the person's particular circumstances, e.g., use of interpreters, etc.

If a patient believes that information held by this practice is inaccurate or incomplete, we will take steps to amend or correct the information.

This practice may refuse access if it reasonably believes that:

- A person's health, safety or wellbeing may be compromised by releasing the information; or
- Providing access would be unlawful or would prejudice a legal investigation.
- Providing access would affect the privacy of others.
- The request for access is frivolous and/or vexatious.
- The information held in the patient's medical record would be used against the doctor in a medico-legal matter.
-

Under circumstances other than those described above where information is withheld, this practice will ensure that its practices are consistent with the provisions of APP 6.
If information is withheld, this practice will provide an explanation to the patient as to the reasons why this was the case.

Procedure

1) Obtain written request from patient using the request to access medical records form (identification must be provided).
2) Inform patient that there may be a fee charged and Medicare does not cover these fees.
3) Request is sent to the patient's usual GP.
4) The doctor will decide whether to disclose the information requested or decline the patient's request.
5) The Practice Manager will acknowledge the patient's request within 14 days of the request.

Please refer to Section 10 – Privacy Request for Access Checklist for the practice's template on handling an information request and the Request to Access Medical Records Form.

1.1 Corrections of Personal Information

APP 13 - Corrections of Personal Information

If you hold personal information about an individual; and you are satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests you to correct the information; you must take such steps (if any) as are reasonable in the circumstances to correct that 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.

Policy

A patient may ask to have their personal health information amended if they considers that is not up to date, accurate and complete. Our practice will try to correct this information. Corrections are attached to the original health record.

Where there is a disagreement about whether the information is indeed correct, our practice attaches a statement to the original record outlining the patients' claims.

It is the policy of this practice that identified errors are not permanently removed. It will be noted in the record that the information has been deemed incorrect, incomplete or not up-to-date, add changes to correct the information and initialled and dated by the author with an explanatory note beside or below the original item. Thus the reason for the incorrect entry is clearly documented with the new entry underneath or in the next available position. The new entry is signed or initialled and dated.

Procedure

The notes containing the error are to be selected in Best Practice

1. The Amend notes button is to be selected and the correction to the notes made and an explanatory note documented. The time and date and author of the correction with automatically be recorded in Best Practice.

2. If required, the Past History, medication list, recalls and reminders or other elements of the medical record are to be corrected at this time.

PART G – COMPLAINTS HANDLING

1.0 Complaints about privacy breeches

Complaints relating to a privacy breech are taken very seriously and may be made by any individual, either as an identified entity or anonymously. Complaints can be made in writing, via phone or in person. The Practice Manager is the first point of contact for a privacy breech complaint. Patients are advised how to make a complaint on the Patient Privacy Policy Form. Once a complaint has been received by the practice manager, the privacy breech report (See section 10) is completed and a response, if required, is provided within 30 days.

If individuals can also contact the OAIC – Office of Australian Information Commissioner (www.oaic.gov.au) on 1300 363 992.

PART H – PERSONAL INFORMATION AND OVERSEAS RECIPIENTS

8.0 APP 8 – 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.

Policy

This practice will only transfer personal information about a patient to someone who is in a foreign country if:

The patient consents to the transfer; and
The recipient is bound by legislation that is substantially like the APPs; or
This practice is reasonably sure that the information will not be held, used, or disclosed inconsistently with the APPs.

PART I INFORMATION SECURITY

9.0 APP 11 Security of Personal Information

Policy

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.

All personal information held by this practice will be:

- If in electronic form, protected from theft, loss, or corruption.
- Accessible by team members only on a "need to know" basis.
- Protected from viewing or access by unauthorised persons; and
- Not taken from this practice site unless authorised and for a specified purpose.

We will destroy or permanently de-identify personal information that is no longer required by this practice.
We will ensure that all personal information transmitted electronically will be appropriately encrypted before transmission.

Procedure

The following guidelines are followed for maintaining security:

Practice records are to be maintained, handled, and stored in a manner which will prevent:

- Loss
- Breaches of confidentiality
- Unauthorised access

Maintain Privacy/Confidentiality from others (e.g., patients, public and team members) under all circumstances including patient:

- Address
- Telephone number
- Results

Written/telephone requests – always follow the correct procedure.
Ensure appropriate disposal of documents including patient files, accounts, and business records.

This practice maintains an accurate recording system to update and track files, especially changes of name or address. Correct disposal requirements must be observed.

Security is always maintained for files.

9.1 Computer

Policy

It is the policy of this practice that data held on the practice's computer system is secured to prevent unauthorised access, exploitation, and loss of data.

Team members, temporary team members and contractors that require access to the practice's systems are required to sign confidentiality agreements before commencing work.

Electronically held data will be protected from exploitation by organisations that may sell the data for commercial purposes. Disks, faxes, and computer printouts are positioned or stored out of sight when not in use.

Computer equipment is in physically secure areas within the practice or is secured by anti-theft and data loss protection devices (lockable cables, drive locks).

9.2 E-mail

Policy

Patient information is only sent via e-mail if it is securely encrypted according to industry and best practice standards. Refer to Section 5 – Computer Administration for more details.

9.3 Facsimile

Policy

The following procedure is to be strictly adhered to, due to the medico-legal nature of our patient information:

When faxing patient information, the fax number and identification of the recipient must be confirmed before transmitting.

Ask the person requesting the fax to ensure that someone authorised is standing by to receive the fax.

Record "Confidential" on the fax coversheet.

Check the number dialled before pressing 'SEND'.

Keep transmission report produced by the fax as evidence that the fax was sent. Also confirm the correct fax number on the report.

PART J – DISPOSAL OF PERSONAL/HEALTH INFORMATION

9.0 If Thrive Medical receives any unsolicited personal information that is not deemed appropriate for the permitted health situation, Thrive Medical will reasonably de-identify and dispose of said information accordingly.

9.1 If Thrive Medical holds any personal or health information that is no longer deemed relevant or appropriate for the permitted health situation, Thrive Medical will reasonably de-identify and dispose of said information accordingly.

PART K – PATIENT PRIVACY POLICY AND ACCESS TO POLICY

9.0 Thrive Medical has a specific patient privacy policy which is attached at 9.9.18. Thrive Medical provides free copies of this Privacy Policy for patients and staff to access, which can be/will be provided upon request. The Patient Privacy Policy is also available on the practice website.

PART L– REVIEW OF POLICY

10.1 Thrive Medical in accordance with any legislative change will review the terms and conditions of this policy to ensure all content is both accurate and up to date annually, with a reminder in KnowNow.

10.2 Notification of any additional review(s) or alteration(s) to this policy will be provided to patients and staff within 1 month notice, via the website. If change occurs patients and staff are required by Thrive Medical to review/sign/acknowledge in writing etc. this Privacy policy.

9.9.18 Thrive Medical Patient Privacy Policy

Thrive Medical Patient Privacy Policy

Current as of: 14/09/2023

Introduction

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties. Thrive Medical is committed to ensuring the privacy and confidentiality of all personal information affiliated with Thrive Medical's business undertakings. Thrive Medical follow the terms and conditions of privacy and confidentiality in accordance with the Australian Privacy Principals (APPs) as per schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, forming part of the Privacy Act 1998.

In this Privacy Policy, common terms and definitions include:

- "personal information" as defined by the Privacy Act 1988 (Cth). Meaning "information or an opinion including information or an opinion forming part of a database, whether true or not, and whether recorded in a material format or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion"; and,
- "health information" as defined by the Privacy Act 1988 (Cth). This is a particular subset of "personal information" and means information or an opinion about:
  - the health or a disability (at any time) of an individual;
  - an individual's expressed wishes about the future provision of health services to them; or,
  - a health service provided or to be provided to an individual.
  -

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information and health information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold and share your personal information?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details , preferred pronouns
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- health fund details.

Dealing with us anonymously

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.

How do we collect your personal information?

Our practice may collect your personal information in several different ways.

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration. Information provided via online patient registration forms, will be added to your electronic medical records.
2. During the course of providing medical services, or registration as a new patient, we may collect further personal information. Information may be collected through electronic transfer of prescriptions (eTP), QScripts, My Health Record eg via Shared Health Summary, Event Summary, QHealth – The Viewer, HPOS and PRODA
3. We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.
4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:
    - your guardian or responsible person
    - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
    - your health fund, Medicare, or the Department of Veterans' Affairs (as necessary).
5. All personal information we be update in accordance to any change in your circumstances that are brought to Thrive Medical's attention. All changes to personal information will be subject to your consent and acknowledgement.

When, why and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties who work with our practice for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers

- when it is required or authorised by law (eg court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (eg via Shared Health Summary, Event Summary), The Viewer, Qscript, HPOS and PRODA.

  Only people who need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Our practice will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying our practice in writing.

Our practice may use your personal information to improve the quality of the services we offer to our patients through research and analysis of our patient data.

We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified, and the information is stored within Australia. You can let our reception staff know if you do not want your information included. Consent for sharing this information for Quality Improvement is obtained on new patient registration.

Personal information for children aged 14 years and below may be shared with parents, at the doctors, discretion and in alignment with any custodial documentation. Children aged 15 years and above, will may choose whom we can share their personal information with and will be provided with a 15+ consent form to be completed after their 15th birthday.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms. We use an electronic medical record as the primary storage for your personal information. We receive medical imaging (x-rays and scans), pathology (blood tests and other tests) and some specialist and allied health communication, through direct computer download which allows us to import them directly to your personal electronic medical record. Any information received in paper format is scanned into your electronic medical record and the original securely destroyed.

You may request that specific Health information is made confidential in your electronic medical record. This will exclude this information being included in summaries or referral letters. We use electronic templates for referrals, consent forms, letters and care plans – information is imported directly from the electronic medical record to these documents. Thrive medical reviews templates to ensure that only appropriate information is contained.

Our practice stores all personal information securely. Electronic medical records are password protected. All information is stored and backed up to a secure local server. All staff, contractors and tenant doctors have signed confidentiality agreements.

What we do if we detect a privacy breech?

If Thrive Medical detects a privacy breech, we will contact you via phone and advise the nature of the breech, what information has been breeched. We will review the circumstances related to breech and

provide feedback to you, as appropriate. Appropriate preventative actions including, but not limited to the following may be undertaken:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of employee training practices, or
- review of contractual obligations with contracted service providers

How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing, using the "Request to Access Medical Records " form that can be located on our website or obtained by contacting our reception staff and our practice will respond within 30 business days. An appropriate, determined suitable by the doctor, to cover the administrative cost of this service, will be charged You will be advised of the applicable fee by administration staff, which is not redeemable under Medicare or private health insurance.

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by our practice is correct and current. You may also request that we correct or update your information, and you should make such requests in writing to manager@thrivemedical.com.au

How can you lodge a privacy-related complaint, and how will the complaint be handled at our practice?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing, via phone or in person. We will then attempt to resolve it in accordance with our resolution procedure. Written complaints can be emailed to manager@thrivemedical.com.au. The practice manager can be contacted by calling the practice on (07) 40192960 and asking to speak with the Practice Manager. If you would like a written or verbal response, you need to provide your address and contact details. Once your complaint has been received by the practice manager, we will provide a response, if required, within 30 days.

If you wish to provide an anonymous complaint this can be mailed to the practice at PO Box 841N, Cairns North or deposited in the mailbox at the front of the practice at 37 O'Keefe Street, Cairns North.

You may also contact the OAIC. Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Privacy and electronic communication

Our practice may communicate with you via SMS or email. As part of new patient registration, you can consent to SMS communication from the practice software. To enable this function, you will be sent an electronic code which you provide to the practice to allow them to activate SMS communication. You can opt out of SMS communication at any time via verbal or written communication.

Our practice may use email to send you copies of referrals, results, forms or other information you have requested. All emails are sent with a PIN code required to unlock, unless you request that it is not sent with PIN protection.

Access to the Thrive Medical Privacy Policy

Thrive Medical provides free copies of this Privacy Policy for patients and staff to access, which can be/will be provided upon request or via our website: www.thrivemedical.com.au

Policy review statement

This policy is reviewed regularly and will be reviewed on 14/09/2024