The Williamstown General Practitioners Group Pty. Ltd.
ABN 27 006 916 098

Dr. V. Vizec (PROV NO: 310894J)
Dr. J. Farrow (PROV NO: 471591J)

HEALTH PRIVACY POLICY AND PROCEDURES

Background
In compliance with the Privacy Amendment (Private Sector) Act 2000, Williamstown General Practitioners Group has prepared this Privacy Policy to describe the way and circumstances under which personal information is collected, stored, used and disclosed by the Practice. The Policy is intended as a guide to general practitioners, practice staff and for the advice of the broader community.

The policy is a public document and access to it will be granted on request.

> *Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.* (p 57 *Guidelines on Privacy in the Private Health Sector,* Office of the Federal Privacy Commissioner)

1. Our statement of commitment:

The doctors and staff of this practice are committed to giving you our valued patient, quality care and service.

All staff are trained in the appropriate handling of personal information by this practice.

We protect your privacy and treat all patient information including health and financial details as private and confidential.

We have developed and documented a privacy policy according to current privacy laws*. Doctors and staff of this practice abide by this privacy policy and understand that a policy breach is grounds for dismissal.

2. Our Privacy Policy states:

What our primary purpose is
What type of personal information we collect
Purpose of collection
How information is collected and stored
How information is used, protected and disclosed
Do we inform patients of the intended use of their information?
Do we obtain a patient's consent?
Is the data we collect accurate, up to date and complete?
How do we protect data from misuse, loss and unauthorised access?
How to access your personal information
How you can make a complaint about a possible privacy breach

* Commonwealth Privacy *Act* Privacy Amendment (Private Sector) Act 2000 Victorian Health Records Act 2000

1. Our primary purpose

Our primary purpose is to provide comprehensive, co-ordinated and continuing whole person medical care for individuals, families and the wide community to the very best of our ability.

2. Type of personal information collected by the practice

Patient identifying details including date of birth, address, telephone, emergency contacts, marital status, employer details, Medicare Number, Health Insurance details, ethnicity, allergies & other sensitivities, past & current medical history, social history, medical procedures, diagnostic tests, results, referrals, reports from other health service providers, radiology films and reports, pathology test results, progress notes, financial details related to billing, medications, immunisations, work cover examinations - dates, amounts, related to this data. Where possible information is collected directly from the patient.

3. Purpose of collection

To gain sufficient information to provide for holistic ongoing management of the patient's health, care and well being and to ensure practice viability in continuing to treat patients.

4. How information is collected and stored

Paper, electronic - patient registration form, accounts form, Medicare, Health Insurance claim form, Referral letter, medical record forms as per Rolls Printing/RACGP medical records. Medication scripts written manually & via computer (Medical Director software), Immunisation forms - ACIR, Pap Smear Registry forms, S8 Drugs - internal booklet used paper form to denote usage, sterilisation register (paper), doctor's letters/referrals on computer or paper. Medical records stored electronically on computer; also old records prior to Jan 1999 stored in paper records. Data accessed only on authorisation of authorised GPs and staff.

Computers have password access with paper medical records stored in restricted filing area. Staff who access files have signed privacy agreements. Practice Manager and Reception staff require access to accounts, demographic records and from time to time actual medical records. GPs are also aware of privacy restrictions and access issues and use passwords for computer access.

5. How information is used, protected and disclosed

For maintaining current information about patients, updating demographics; accounts - payment, invoicing, follow-up; recall & reminder system, actioning report results, adding to medical record for comprehensive data - results, operation reports, emergency department visits, after hours & home consultations, telephone notes,
For primary purpose and related secondary purpose: GPs, Practice Manager, Reception staff.
Account details will only be provided to gain payment from insurance/Medicare office. No additional unnecessary data will be given. Pathology/Radiology, other medical, dental specialists, and allied health service providers included here.
Transfer of files – This Practice will obtain a written request from the patient. GP will maintain a copy of the completed patient request form. Provide clear details of the form of release of the patient file.
If research is being conducted, then each patient provides informed consent for his/her personal health information to be released. Patient has right to access own personal health information under privacy legislation with noted exceptions. See our policy and NPP6 Access & Correction.

Under certain legislation we must disclose patient information eg. Infectious Diseases Act - Health (Infectious Diseases) Regulations, Adoption Act.
Records must be disclosed under court orders, subpoenas, search warrants and Coroner's Court cases.

6. Do we inform patients of the intended use of their information?

If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, patient informed consent may be obtained;

Individuals will be given the opportunity to refuse such use or disclosure.

If an individual 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 individual's or the public's health and safety.

Information may be disclosed to a responsible person (as described under the Act). We will keep records of any such use and disclosure.

7. Do we obtain a patient's consent?

Personal information for disclosure to a third party will only be provided with the patient's informed consent, or where you expect such disclosure, or where we are legally required or authorised to do so.

8. Is the data we collect accurate, up to date and complete?

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.

9. How do we protect data from misuse, loss and unauthorised access?

This Practice will 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 paper form, received and stored in a secure, restricted location;
- if in electronic form, password and firewall protected;
- accessible by staff only on a "need to know" basis;
- not taken from the Practice unless authorised and for a specified purpose.

We will destroy or permanently de-identify personal information that is no longer required by the Practice.

10. How to access your personal information

10.1 Under normal circumstances this Practice will provide an individual with access to their personal information within 30 days of receiving a request for access.

10.2 There will be no fee associated with lodging a request for access, however, a small but reasonable administration fee may be charged.

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

10.4 If an individual believes that information held by the Practice is inaccurate or incomplete, the Practice will take steps to amend or correct the information.

10.5 The Practice may refuse access if it reasonably believes that:

10.5.1 A person's health, safety or wellbeing may be compromised by releasing the information; or

10.5.2 Providing access would be unlawful or would prejudice a legal investigation.

10.6 Under circumstances other than 10.5.1 and 10.5.2 where information is withheld, the Practice will ensure that its practices are consistent with the provisions of NPP 6.

If information is withheld under 10.5.1, the Practice will provide an explanation to the individual as to the reasons why this was the case.

12. How you can make a complaint about a possible privacy breach

12.1 Any complaints in relation to this Practice's handling of personal information should be directed to the Privacy Officer (Principal Doctor or Practice Manager). In most cases the complainant will be asked to lodge their complaint in writing.

12.2 Unless a complaint can be dealt with immediately to the satisfaction of both parties, the Practice will provide a written response to the complaint within 30 days of its being received.

12.3 If an individual believes their complaint has not been appropriately handled by the Practice, they should contact the Office of the Federal Privacy Commissioner, Privacy Hotline 1300 363 992 (local call charge) or via www.privacy.gov.au

WILLIAMSTOWN GENERAL PRACTITIONERS GROUP PTY. LTD.

Staff Privacy Statement

Procedure

In accepting employment at this practice the confidentiality policy will be explained to the new employee by the Practice Manager or Principal and a privacy statement will be signed.

Original retained in staff personnel file and a copy given to the staff member.

1. _____ I have read and understood the Practice Policy and Procedure Manual. I understand this practice's requirement to protect the privacy of its information, in particular: patient records including clinical data, accounts, verbal discussions, written documents including those emanating from computers or facsimile machines heard, written, received or otherwise produced by others or myself are deemed strictly private and confidential and are not to be discussed or in any way released to anyone except under instruction by the Practice Principal or designate and according to privacy law*.

I understand that a breach of this policy is grounds for immediate dismissal.

Staff Name _____

Staff Signature _____

Date _____

Principal Name _____

Principal Signature _____

Date _____

* Commonwealth Privacy Act - Privacy Amendment (Private Sector) Act 2000

* **Victorian Health Records Act 2001**

Procedure in processing of a request to access personal health information

A patient may make a request verbally at the practice, via telephone or in writing e.g. fax, email or letter. No reason is required to be given. The patient's doctor, reception or other staff, Privacy Officer or health service provider at this practice can receive a request for access.

To ensure correct processing of the request, complete a **Request for Personal Health Information form**. See sample in this section. The form asks patients to write their name and related details; what type of access they require and to specify where possible what information, they seek. Staff member to complete remaining sections and place a record of the request in the Access Register.

Also write every request received on a summary form that serves as a request register.

Request by another person (not the Patient.)

An individual may authorise another person to be given access, if they have the right e.g. legal guardian and if they have a signed authority. Under NPP 2 Use & Disclosure, a 'person responsible' for the patient (including a partner, family member, care, guardian or close friend), if that patient is incapable of giving or communicating consent, may apply for and be given access for appropriate care and treatment or for compassionate reasons. Identity validation applies.

The Privacy Act defines a 'person responsible' as a parent of the individual, a child or sibling of the individual, who is at least 18 years old, a spouse or de facto spouse, a relative (at least 18 years old) and a member of the household, a guardian or a person exercising an enduring power of attorney granted by the individual that can be exercised for that person's health, a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency

Children

Where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so according to Federal Privacy Commissioner's Privacy Guidelines. The doctor could discuss the child's record with their parent. Each case is dealt with subject to the individual's circumstances. A parent will not necessarily have the right to their child's information.

Deceased Persons

A request for access may be allowed for a deceased patient's legal representative if the patient has been deceased for 30 years or less and all other privacy law requirements have been met. Ref: Sec 28 Health Records Act. No mention is made of deceased patient's access in Commonwealth privacy legislation.

Methods of Access

Personal health information may be accessed in the following ways:

- View and inspect information
- View, inspect and talk through contents with the doctor
- Take notes
- Obtain a copy (can be photocopy or electronic printout from computer)
- Listen to audio tape or view video
- Information may be faxed to patient after making sure the person requesting access, is directly receiving the fax at the other end

Check Identity of Patient

- Ensure a visible form of ID is presented by the person seeking access. E.g. driver's licence, passport, other photo identification. Note details on request form.

- Does the person have the authority to gain access? Check age, legal guardian documents

Acknowledge Request

Each request is to be acknowledged. For a verbal request, it can be done at the time of request or if in writing, then a letter is sent to the patient, confirming request has been received. Send letter within 2 working days if possible or within 14 days as recommended by the National Privacy Commissioner. Acknowledgment will include a statement concerning charges involved in processing request.

Fees Charged

No recommended fees have been set by the National Privacy Commissioner and generally minimum fees, if necessary are to be charged. However, the following costs are charged to the patient or other legitimate applicant for processing a request.

Search & Retrieval	$20 (includes assessment & collation of data)
Inspection	*$5-00* per 15 minutes
Photocopying	$20c per A4 page
X-Rays	Facility not available

Based on *Draft Proposal for Health Records Regulations Reg. 5*
Maximum Fee for Granting an Individual Access to Health Information.
Victorian Health Records Act, Nov 2001

Collate & Assess Information

Retrieve patient's hardcopy medical record or arrange for the treating doctor or practice principal to access the computer record. Attach patient request from for doctor to assess what information is be given to the patient.

On occasion some data may be withheld under privacy legislation NPP6 Access & Correction e.g.

- Where access would pose a serious threat to the life or health of any individual
- Where the privacy of others may be affected
- If a request is frivolous or vexatious
- If information relates to existing or anticipated legal proceedings
- If access would prejudice negotiations with the individual
- If access would be unlawful
- Where denying access is required or authorised by law

See National Privacy Principles in full details for full list of exclusions.

Access Denied

Reasons for denied access must be given to the patient. Note on request form. In some cases only a small portion of information may be denied to the patient but all other data must be given as per request.

Use of Intermediary When Access Denied

lf request for access is denied an intermediary may operate as facilitator to provide sufficient access to meet the needs of both the patient and the doctor. For more detail see p.37 of Guidelines on Privacy in the Private Health Sector.

Any Information to be Deleted/Removed?

Where the doctor considers that information should be deleted or removed from the record then this is to be done and noted on record form. it may be useful for the doctor to document any 3rd party information nor for future release, on a separate sheet or section of the computer.

Paper based information can be deleted with black felt pen and then photocopied (twice if needed) to remove any possible reference to prior data.

Provide Access

Patient may view information, take notes and have a copy given to them, if the patient is viewing the data, seat them in the room adjacent to the practice manager's office or in the quiet area next to reception.
Supervise each viewing so that patient is not disturbed and no data goes missing.

If a copy is to be given to the patient ensure all pages are checked and this is noted in the request form.

If the doctor is to explain the contents to a patient then ensure an appointment time is made.

Requests to Correct Information

A patient may ask to have their personal health information amended if he/she considers that is not up to date, accurate and complete. (NPP 6.5/6/6)

Our practice must 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 patient's claims.

Time Frames

Acknowledge request within 14 days but try for 2 working days.
Complete request within 30 days

WILLIAMSTOWN GENERAL PRACTITIONERS GROUP PTY. LTD.
Suite 2, 81 Ferguson St., Williamstown 3016
Ph: (03) 9397 7300 Fax: (03) 3937 3011

REQUEST FOR PERSONAL HEALTH INFORMATION

1. Patient Details (Please print in BLOCK LETTERS)

Surname _____

Given Name/s _____

Address _____

_____

Date of Birth _____

2. Health Information Requested: Please √ tick box

☐ Blood Test Results. Most recent? Y/N or specify date/s _____

☐ X-Ray Results. Most recent? Y/N or specify date/s _____

☐ Other Test Results. Please specify _____

☐ A Summary of My Health Record

☐ Health Record

☐ Other. Please give details _____

_____

_____

_____

_____

3. How Would You Like To Receive This Information?

☐ View and inspect information. I will make a time with reception.
☐ View, inspect & talk through contents with my doctor, 1 will make an appointment at reception.
☐ Obtain a copy
☐ Obtain a copy - Please send it to me via mail
☐ Obtain a copy - Please fax to me at Fax No _____

An access fee will be charged according to the amount of information requested and the time taken to retrieve it.

Signature of Applicant _____ Date _____

_____ Office Use Only	Staff to initial & date each entry
☐ Date request received_____	
☐ Acknowledged date _____	
☐ Personal ID sighted licence/passport/other, _____	
☐ Pension or Health Care Card Y/N	
☐ Appointment made with doctor? Y/N Date & Time _____	
☐ Patient to collect Expected Date -	
☐ Doctor advised	
☐ Noted in patient record	
☐ Record checked & ready for patient	
☐ Data Removed/deleted Y/N	
☐ Method of access: View/View & Dr/Copy & collect/Copy & send	
☐ Fee Charged? Y/N Amount $ (excl GST) Fee Received $	
☐ Access process complete (record viewed/sent) Date	

Privacy Audit

Policy

From time to time or at least every 3 years and according to privacy law and guidelines, this practice conducts a review of privacy policies and procedures.

Procedure

The Privacy Officer reviews the following items:

- What is the primary purpose of this practice?
- What data do we collect and document? NPPI/HPP1
- How do we store this information? NPP5
- What data do we disclose and to whom? NPP2
- When and how do we obtain patient's consent? NPP2/HPP2

Information is collected from hard copy and electronic storage devices and issues discussed with GPs and staff to gain the most current information.

National and state privacy laws are referenced with any updates being noted and acted upon.

Policy Manual. Patient Access Forms/Register Brochures and Poster

At this time the Practice policy & procedure manual may be reviewed and updated for privacy items, if not already done.

Forms related to 'Patient Access to Health Information," including request for access and access register forms can also be reviewed at this time.

Detailed patient privacy brochures, stating our practice privacy policy in general as per privacy legislation is reviewed and updated as necessary. Obtain additional copies or re-print as needed.

A3 general patient privacy wall poster, advising patients of our privacy policy is reviewed and updated as necessary.

Ref: Guidelines on Privacy in the Private Health Sector; Office of the Federal Privacy Commissioner Oct 2001.

NATIONAL PRIVACY PRINCIPLES

adopted within Privacy Amendment (Private Sector) Act 2000
Commonwealth Privacy Act
Effective 21 December, 2001

Personal information in an organisation

1. Collection	2. Use & disclosure	3. Data quality
4. Data security	5. Openness	6. Access & correction
7. Identifiers	8. Anonymity	9. Transborder data flows
10. Sensitive data		

NPP 1 Collection
- Must be lawful, fair & not intrusive
- Person must know ID of organisation & how to contact: know can access info, purposes for collection, types of organisations to which information will be disclosed, laws about info collection, consequences if info not provided by person
- If reasonable & practical obtain information from actual person

NPP 2 Use & Disclosure
- Consent to use/disclose only for purpose it was collected or in circumstances related to public interest e.g. law enforcement, public/individual health & safety. Make written note of disclosure. If related to primary purpose & is secondary & non-sensitive e.g. marketing in specified cases & individual would reasonably expect the org. to use or disclose the info. Responsible individual may disclose (parent, child or sibling min. 18 yrs, spouse, relative, guardian, enduring power of attorney, person with intimate relationship, person nominated by individual)

NPP 3 Data Quality
- Organisation must take reasonable steps that personal info it collects, uses or discloses, is accurate, complete & up to date.

NPP 4 Data Security
- Organisation must take reasonable steps to protect info from misuse, loss and unauthorised access, modification or disclosure.
- Destroy or permanently de-identify data if no longer needed

NPP 5 Openness
- Must document policy an management of personal info. & make available to all who ask
- If asked what info held: purpose, how collected, held, used & disclosures

NPP 6 Access and Correction
- Access on request by individual except where access would pose: serious & imminent threat to life or health of any individual, or impact unreasonably on privacy of other individuals, frivolous/vexatious, if relates to existing or anticipated legal proceedings, be unlawful, could prejudice process of criminal investigation, where protects public revenue, cause damage to OZ security
- If org. charges for access - must not be excessive & not apply to request for access
- Can correct data that is not accurate, up to date & complete
- if disagree re previous point then must be documented
- Denial of access - organisation must provide reasons and also if it does not wish to correct info.

NPP 7 Identifiers
- In general organisation must not use ID that Government agency uses (Tax File, Medicare)

NPP 8 Anonymity
- Organisations must give people option to interact anonymously whenever it is lawful & practical

NPP 9 Transborder Data Flows
- Transfer of data to foreign country where individual consents or where info held, used etc. as per NPPs.

NPP 10 Sensitive Information

- Sensitive data only collected if consent given or required by law or to protect individual who is physically / legally incapable of giving consent
- Data can be collected if necessary to provide a health service to individual & data collected by law or with rules of competent health / medical bodies that deal with obligations of professional confidentiality which bind the organisation
- Data can also be collected for research / stats relevant to public health or safety, compiling and for all these & previous point it is impracticable to seek individual consent & data is collected as required by law & in accordance with rules of competent health or medical bodies etc. & must take reasonable step to de-identify data prior to disclosure

National Privacy Principles 2000. Go to www.privacy.gov.au for more details, guidelines and latest updates.