Glenelg Health Care – Management of Patient Health Information Policy

This policy is to address the management of 'personal health information in our practice.

This Policy: Is written from the template provided by the RACGP for use in general practice Is based on the handbook for the management of health information in Private medical practice.

Is consistent with the national privacy principles for the fair handling of personal information in the federal privacy act 1988.

This policy incorporates but is not limited to, the patient health record, Medicare and DVA billings and accounting records, pathology results, medical certificates, incoming and outgoing correspondence from hospitals, other doctor, and allied health professionals.

Privacy

Personal health information is defined as information concerning a patient's health, medical, history, or past or present medical care; and which is in a form that enables or could enable the patient to be identified. It includes information about an individual's express wishes concerning and current and future health services.

All GPs and practice staff must ensure that the patient can discuss issues relating to their health, and that the GP can record relevant personal health information in a settng that provides visual privacy and protects against any conversation being overheard by a third party.

Staff will not enter consultation room during a consultation without knocking or otherwise communicating with the GP.

Staff, registrars, and students will not be present during the consultation without the prior permission of the patient. Patient will give consent for a third party to be present.

Where possible, any distressed patients will be offered to wait in a spare room or private area away from others before of after their consultation.

Privacy Officer

Glenelg Health Care has appointed Jancine Lee, our practice manager as the Privacy officer who is responsible for formulating and implementing, monitoring, and promoting our privacy policy. Upon request Glenelg Health Care supplies our patients either verbally or via a hard copy of our practice's policy regarding the collection and management of their personal health information. They are informed they can request it on our practice website and our patient information leaflet.

Informing New Patients

GPs and our practice nurse are able to discuss the practice's privacy policy with patients who are new to the practice at their first visit or when it is clear that the patient is continuing at the practice. New patients will be offered the practice's information leaflet informing them we about their personal information and their privacy and will be offered access to the Management of Health Information Policy. Glenelg Health Care tries to make sure that the information on privacy is available to patients is appropriate for the range of people who come here. Feedback about the information is always welcome.

Practice staff will ensure that current information about the practice's approach to personal privacy are available at the reception desk.

Patient access to their personal health information

Under privacy legislation provisions, all patients have the right to access their health information stored at the practice. The treating GP will provide an up to date and accurate summary of their health information on request or whenever appropriate.

The treating GP will consider all requests made by a patient for access to their medical record. In doing so the GP will need to consider the risk of any physical or mental harm resulting from the disclosure of health information.

If the GP is satisfied that the patient may safely obtain the record then he/she will either show the patient the record, or arrange for provision of a photocopy, and explain the contents to the patient.

Any information that is provided by others (such as information provided by a specialist or other practitioner) is part of the health record and can be accessed by the patient. Occasionally the patient may be referred by the treating specialist for access to their letters. Appropriate administration costs may be charged to the patient.

Alteration to Patient Records

Glenelg Health Care will alter personal health information at the request of the patient when the request for alteration is straight forward (e.g. changing a mobile number or email address)

With most requests to alter or correct information, the general practioner will annotate the patients record to indicate the nature of the request and whether the GP agrees with it. For legal reasons, the doctor will not alter or erase the original entry.

Access to personal health information by staff for the purpose of research, professional development, and quality assurance/improvement.

New patients will also be informed that the practice undertakes quality improvement activities from time to time to improve individual and community healthcare and practice management.

Patients will be advised of the ways in which the practice undertakes "recall" and "follow up" activities e.g. when the practice would phone, SMS or write to a patient. Consent is gained from the patient to participate in a recall or reminder system via the new patient details form and the update details form.

Should this general practice decide to stop a recall or reminder system, it will write to each person on the system at their last known address and advise them that the system will be ceasing.

Patents will be informed when quality improvement activities will be conducted and given the opportunity to "opt out" of any involvement in these activities. The GP responsible for the activities will ensure that appropriate information is available to patients from the reception staff.

Glenelg Health Care wll only participate in quality improvement and clinical audit activities associated with de-identified data. If the practice does decide to participate in any research activities in the future, then the practice will ensure that they follow all legal and ethical

responsibilities outlined in the RACGP - Three key principles for the secondary use of general practice data by third parties.

This Includes: •

- All parties must demonstrate compliance with data management best practice.
- All parties will act ethically regarding the practice data.
- Data must only be used for agreed purposes.
- Data security is everyone's responsibility.
- Special considerations apply for data linkage.

Healthcare consumers will have transparency and agency in the use of their health data.

- Glenelg Health Care will provide information on secondary use to patients.
- Glenelg Health Care will provide patients an opportunity to opt out of providing data for secondary use to patients.
- Consent will be obtained from patients for particular secondary uses.
- Special considerations will apply data on or about Aboriginal and Torres Strait Islander peoples.
- Special considerations will apply for data on or about other patient groups in particular significance.

The contribution from Glenelg Health Care will be valued and recognised.

- Glenelg Health Care will retain access and control over what can be extracted.
- There will be a value proposition for Glenelg Health Care
- GP advisors will be involved in data analysis and interpretation.

Confidentiality Agreement's

In order to protect personal privacy, this practice has all staff, including temporary or casual staff; Subcontractors (e.g. software providers etc) and medical students sign a confidentiality agreement.

Disclosure to Third Parties

GP's and staff will ensure that personal health information is disclosed to third parties only where consent of the patient has been obtained. Exceptions to this rule occur with the disclosure is necessary to manage a serious and imminent threat to the patient's health or welfare or is required by law (Subpoenas).

The GP will refer to relevant legislation and the maturity of the patient before deciding whether the patient (in this case a minor) can make decisions about the use and disclosure of information independently (i.e. Without consent of a parent or guardian). For example, for the patient to consent to treatment, the GP must be satisfied that the patient (a minor) is aware and able to understand the nature, consequences, and risks of the proposed treatment. This patient is then also able to make decisions on the use and disclosure of his or their health information.

GP's will explain the nature of any information about the patient to be provided to other people, for example, in letters of referrals to hospitals or specialists. The patient consents to the provision of this information by agreeing to take the letter to the hospital or specialist, or by agreeing for the practice to send it.

Increasingly there is an expectation by patients that they will see and be advised of the contents of referral letters. They are able to access such letters via the GP. GP's and staff will disclose to third parties only that information which is required to fulfil the needs of the patient.

These principles apply to the personal information provided to a treating team (for example, a consultant physician or allied health who is also involved in the patients care). The principles also apply where the information is transferred by other means, for example, via an intranet. Information classified by a patient as restricted will not be disclosed to third parties without explicit consent from the patient. GP's will make a contemporaneous note when such permission is given.

Information disclosed to Medicare or other health insurers will be limited to the minimum required to obtain insurance rebates.

Information supplied in response to a court order will be limited to the matter under consideration by the court unless entire record has been subpoenaed.

From time-to-time general practitioners will provide their medical defence organisa5on or insurer with information, in order to meet their insurance obligations.

The practice participates in practice Accreditation, which assists us improve the quality of services. Practice accreditation may involve the 'surveyors' who visit the practice reviewing patient records to ensure that the appropriate standards are being met. Glenelg Health Care will advise patients when practice accreditation is occurring by placing a notice in the waiting room prior to the survey visit occurring. Patients will be given the opportunity of refusing accreditation surveyors access to their (the patient's) health information.

Request for Personal Health Information and Medical Records by Other Medical Practices

Access to accurate and up to date information about the patient by a new treating GP is integral to the GP providing high quality health care.

Glenelg Health Care engages an after-hours service to provide care and ensures that this service has emergency contact details for the patients usual GP. A copy of the afterhours consultation is faxed to our practice as soon as practicable and scanned into the patient's health record.

If a patient transfers away from the practice to another GP, and the patient requests that their medical records be transferred, the existing GP will provide a summary to the new treating GP or to the patient. This practice will retain original documents and records.

Glenelg Health Care will seek written permission from the patient for the provision of personal health information to another medical practice. This permission will be scanned into the patient's health record. If the patient wishes to transfer their entire medical records, then an administrative fee will need to be paid prior to the patients file being imported onto a disk and sent via registered post to the new treating GP practice. (Fee is dependant on the size of the information being requested).

Security

Medical practioners, practice staff and contractors will protect personal health information against unauthorised access, modifications or disclosure, misuse, and loss while it is being stored or actively used for continued management of the patient's health care. Staff will ensure that patients, visitors, and other healthcare providers to the practice do not have unauthorised access to the medical record storage area or computers.

Staff will ensure that records, pathology test results, and any other paper or electronic devices containing personal health information are not left where unauthorised persons may access them.

Non-Clinical staff will limit their access to personal health information to the minimum necessary for the performance of their duties.

Fax, email, and telephone messages will be treated with security equal to that applying to medical records.

Computer screens will be positioned to prevent unauthorised viewing of personal health information. Through the use of, for example, password-protected screen savers, staff will ensure that computers left unattended are locked and cannot be access by an unauthorised persons. GP's, nurses, and admin staff will ensure that personal health information held in the practice is secured against loss or alteration of data.

Patient records will not be removed from the practice, except when required by clinical staff for patient care purposes. Records will be kept securely while away from the practice and the responsible clinician will ensure that records are returned to the practice and left in an appropriate place for filing.

Staff will ensure that manual and electronic records, computers, and other electronic devices and filing areas are secured at the end of each day and that the building is locked when leaving. The data on the computer system will be backed up daily and a duplicate back up is taken off site. Backups are routinely tested to ensure daily duplication processes are valid and retrievable.

Complaints about Privacy-related Matters

Complaints about privacy-related matters will be addressed the same way as other complaints. The procedure for this is outline in our complaints policy.

Retention of Medical Records

It is the policy of Glenelg Health Care that individual patient medical records be retained until the patient has reached aged 25 for a minimum of 7 years from the last time of contact, whichever is longer. No record will be destroyed at any time without permission of the treating GP or of the authorised GP in the practice.

In the event of a GP transferring out of the practice, the practice may post a notice in the practice waiting room, or a GP who is leaving the practice may write individually to each patient, asking them to nominate a practitioner to whom the record should be transferred.

If the practice closes, patents will be contacted individually or, if this is not practical, a public notice will be placed on our website, front door and in the local newspaper, indicating how patients may arrange for their record to be transferred to another GP.

In the event of the practice closing, it has been arranged that any medical records not transferred will be stored securely on our server under the supervision of the practice principal.

Staff training

All staff will receive training during induction, of the practices health record policy. Changes to legislation will be monitored by the practice and passed onto staff and patients as deemed appropriate.