6.1 Privacy and Security of Personal Health Information

Policy

This practice is bound by the *Federal Privacy Act 1998* and National Privacy Principles, and also complies with the *New South Wales Health Records and Information Act 2004*.

'Personal health information' is a particular subset of personal information and can include any information collected to provide a health service.

This information includes medical details, family information, name, address, employment and other demographic data, past medical and social history, current health issues and future medical care, Medicare number, accounts details and any health information such as a medical or personal opinion about a person's health, disability or health status.

All patient health information is considered private and confidential. Disclosure of patient health information is not conducted without the consent of patient's and the GPs. Any information disclosed without consent will result in disciplinary action and possible dismissal of staff.

All staff working within the practice have signed confidentiality agreements as conditions of their employment. Information security is discussed at staff induction and continued education occurs throughout employment.

When patient health information is computerised, electronic measures have been taken to ensure the safety and security of this information. The person responsible for Information Technology/Information Management (IT/IM) is the *Practice Manager in conjunction with Parvis Computers the practice contracted IT providers* who is charged with the coordinating, implementing and monitoring these measures.

Our practice complies with both state and federal privacy legislation relating to medical records. Our practice also complies with the National Privacy Principles.

For each patient we have an individual patient health record containing all clinical information held by our practice relating to that patient. The practice ensures the protection of all information contained therein. Our patient health records can be accessed by an appropriate team member when required. We also ensure information held about the

patient in different records (e.g., at a residential aged care facility) is available when required.

The practice clinical software is Best Practice which uses nationally recognised medical vocabulary. The General Practitioners and Registered nurses utilising are aware of the importance and benefits to the practice when coding patient health information. Correct coding assists with data extraction that helps to identify areas that the clinic can improve patient health care and support quality improvement initiatives.

Procedure

In our practice, patient health information is kept *in our practice software Best Practice* using electronic filing system.

In our practice, the following measures are taken to ensure the security and privacy of patient health information kept as paper records: (time permitting all paper files will be transferred to clinical computerised clinical record in the way of scanning and original files to be discarded in confidential waste.)

- files are stored in a secure room onsite locked after hours (Practice manager room).
- files are stored in area where constant staff supervision can easily be afforded
- files are stored in an area that restricts public access
- files are placed out of view from the patient either face down or behind desks in high patient traffic areas

For records stored electronically, the following procedures are in place to protect patient health information:

- all staff have individual logins and passwords
- staff have restricted levels of access to patient health information depending on their role
- computer screens are located in positions where patient view is obstructed or blocked
- screensavers and automated computer locks are activated during periods of inactivity
- appropriate firewalls and antivirus software is installed and updated regularly
- all information electronically communicated is done so using an encrypted network.

Our practice policy has a documented privacy policy for the management of patient health information which is available to patients upon request and displayed within the waiting area or in the Practice Information Sheet. The policy outlines the following:

- practice contact details
- what information is collected
- reason for the information to be collected
- how the security of information is maintained
- range of people who may access the information
- procedures for access, transfer and disclosure to a third party
- contact details if they believe there has been a privacy breach with their information

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing or in electronic form, except for strictly authorised use within the patient care context at the practice or as legally directed.

Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction including shredding or security bin. Electronic information is securely destroyed using appropriate electronic equipment and processes.