Privacy Statement

This practice is bound by the Federal Privacy Act 1998 and Australian Privacy Principles. 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.

Our practice has a designated person (Dr Frank Simonson) with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security policy (Refer 6.1.1).

Our Security policies and procedures regarding the confidentiality of patient health records and information are documented and our practice team are informed about these at induction and when updates or changes occur.

For each patient we have an individual patient health record (paper, electronic or a combination of both, "Hybrid") 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.

6.1.1 Computer Information Security

Policy

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Doctors and staff are trained in computer use and our security policies and procedures and updated when changes occur.

Dr Frank Simonson has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

All clinical staff have access to a computer to document clinical care. For medico legal reasons, and to provide evidence of items billed in the event of a Medicare audit, staff, especially nurses always log in under their own passwords to document care activities they have undertaken.

Our practice ensures that our practice computers and servers comply with the RACGP computer security checklist and that:

- computers are only accessible via individual password access to those in the practice team who have appropriate levels of authorisation.
- computers have screensavers or other automated privacy protection devices which are enabled to prevent unauthorised access to computers.
- servers are backed up and checked at frequent intervals, consistent with a documented business continuity plan.
- back up information is stored in a secure off site environment.
- computers are protected by antivirus software that is installed and updated regularly
- computers connected to the internet are protected by appropriate hardware/software firewalls.
- we have a business continuity plan that has been developed, tested and documented.

Electronic data transmission of patient health information from our practice is in a secure format.

Our practice has the following information to support the computer security policy:

- current asset register documenting hardware and software including software licence keys
- logbooks/print-outs of maintenance, backup including test restoration, faults, virus scans
- folder with warranties, invoices/receipts, maintenance agreements

This Practice reserves the right to check individual's Computer System history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the Practices Computer Systems or breaches of Practice Computer Security will be fully investigated and may be grounds for dismissal.
This practice has a sound backup system and a contingency plan to protect practice information in the event of an adverse incident, such as a system crash or power failure. This plan encompasses all critical areas of the practice's operations such as making appointments, billing patients and collecting patient health information. This plan is tested on a regular basis to ensure backup protocols work properly and that the practice can continue to operate in the event of a computer failure or power outage.

6.1.1 Computer Information Security

National Privacy Principle 5 requires our practice to have a document that clearly sets out its policies on handling personal information, including health information.

This document, commonly called a privacy policy, outlines how we handle personal information collected (including health information) and how we protect the security of this information. It must be made available to anyone who asks for it and patients are made aware of this.

The collection statement informs patients about how their health information will be used including other organisations to which the practice usually discloses patient health information and any law that requires the particular information to be collected. Patient consent to the handling and sharing of patient health information should be provided at an early stage in the process of clinical care and patients should be made aware of the collection statement when giving consent to share health information.

In general, quality improvement or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment or service would be considered a directly related secondary purpose for information use or disclosure so we do not need to seek specific consent for this use of patients' health information, however we include information about quality improvement activities and clinical audits in the practice policy on managing health information.

(Refer Section 8 Accreditation and Continuous Improvement)