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.

An external contracted provider, Commuserv has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

All clinical staff has 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:

IT SECURITY

- all access to the computer system is controlled via passwords; no information can be accessed without a valid username/password.
- within Medical Director there is a separate user/password system that limits the level of access to patient information to a level deemed appropriate for that login's role within the practice; Medical Director cannot be accessed without a valid username/password combination, even if the computer has been successfully logged into.
- Staff are trained to log out of Medical Director when leaving a computer unattended
- Automatic session locking with password to unlock are provided where required
- Antivirus software is installed on every computer and managed and monitored remotely by Commuserv. Monitoring of critical infrastructure is performed on a real time 24/7 basis. Any detected issues are automatically addressed and if unable to be resolved, are brought to the attention of the practice manager immediately.
- Windows and third party software security updates are managed and monitored remotely by Commuserv. Monitoring is performed on a real time 24/7 basis. Any detected issues are automatically addressed and if unable to be resolved, are brought to the attention of the practice manager immediately.
- Computers accessing the Internet are protected by a hardware firewall device.

BACKUPS

- Backup of the main offsite servers at 380 Grange Road, Kidman Park SA 5025 is carried out by Datto backup appliance in the same location as the servers and this replicates continuously to Datto's main data centre. There is infinite retention of the data centre based backups. Each server is backed up at least twice daily by the Datto appliance. The backup system is autonomous ad alerts are sent to Commuserv and the Practice Manager if there is a backup failure. In addition, a weekly backup report is sent to the Practice Manager.

.

BUSINESS CONTINUITY

- Commuserv have an IT 'disaster recovery' plan in place to ensure business continuity should a major system failure, theft or other disaster occur.
- A full 'disaster recovery' test of the backup system is performed yearly and a written report provided by Commuserv.

SECURE COMMUNICATIONS

- Achieved within the 'Medical Objects' secure email system and secure software provided by external service providers e.g. pathology and radiology results downloads.
- Connection to the cloud servers is by secure VPN link.

DATA DESTRUCTION

- Any retired IT equipment that could potentially contain patient information is sent to Commuserv for secure erasure and destruction. Hard drives are removed from systems, erased using a hard disk wiping utility and either repurposed within the practice, or, if disposed, physically destroyed by mechanical destruction (Smashed with a hammer!).
- USB Sticks and other portable media are erased after use.
- CD's, DVD's are shredded after use.
- Write access to portable media is restricted to only the systems that require it.

PROCEDURE

Our disaster Box stocked with items to enable the practice to operate in the event of a power failure is located in the file room.

- torches.
- paper prescription pads/sick certificates etc.
- appointment schedule printout and manual book.
- letterhead.
- consultation notes.
- manual credit card/payment/Medicare processing equipment.
- emergency numbers.

Doctors rooms have a small package containing:

- a script pad
- patient encounter form

SUPPORTING INFORMATION FOR THE COMPUTER SECURITY POLICY

- Current asset register documenting hardware and software including software licence keys
- Datto backup reports weekly
- 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.