Strathmore Family Medical Centre

Computer Information Security

Policy and Procedures

The Royal Australian College of General Practitioners (RACGP) *Standards for general practices*, 5th edition, indicators state:

- C6.4A – Our practice has a team member who has primary responsibility for the electronic systems and computer security.
- C6.4B – Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.
- C6.4C – Our practice's clinical software is accessible only via unique individual passwords that give access to information according to the person's level of authorisation.
- C6.4D – Our practice has a business continuity and information recovery plan.
- C6.4E – Our practice has appropriate procedures for the storage, retention and destruction of records.

The aim of this policy is to accomplish the requirements of the above indicators and provide a structured approach to our practice's legal obligations, whilst maintaining the security of computers and other devices.

Computer security coordinator

Our practice has a designated computer security coordinator who is responsible for the practice's electronic systems and computer security.

This person is the practice Manager

The duties of the computer security coordinator are documented in their position description.

In this leadership role, the computer security coordinator will have the skills required to undertake the duties and responsibilities required for the position as follows:

- Have medium to advanced knowledge of relevant computer operating systems (e.g. Windows) and the relevant application software.
- Where identified, undergo additional external training in order to fulfil and maintain the duties of the role.
- Have demonstrated management skills to be able to develop practice computer security policies and procedures.
- Keep up to date with relevant legislation, including the Privacy Act and Australian Privacy Principles.
- Monitor, regularly update and review this policy on a quarterly basis.
- Determine when it is appropriate to engage and initiate the services of the practice's external IT support provider for specific support.
- Oversee the commissioning of the practice's external IT support provider to undertake the computer security risk assessment on a yearly basis or when there are system changes.
- Determine when it is appropriate to bring matters of concern to the practice principal.
- Maintain a documented backup procedure and regularly test the process to ensure the data can be restored promptly if there is an incident (e.g. server failure).
- Ensure regular monitoring of system logs and audit reports.
- Ensure that antivirus/anti-malware software and firewalls are installed on all computers and are regularly (automatically if possible) updated.
- Oversee password management and screen security on a regular basis (e.g. every 3 to 6 months).
- When team members terminate their employment, ensure all practice-related accounts are disabled, remote access is disabled, and computer equipment, devices and back-up media are returned.
- Ensure team members are utilising secure messaging delivery for transferring confidential information.
- Maintain the IT assets register (hardware, software, mobile devices, licences, and manuals) that is located:
- Ensure all data breaches are recorded in the electronic incident log, documenting the cause, the response and remedial action taken. Ensure the episode is shared with all team members.

- Oversee IT business continuity and information recovery processes.
- Maintain the storage of physical digital disks and record all associated details, including serial numbers, expiry dates (if applicable) and applicable computers in the asset register.
- Raise awareness and provide training, backup and support in computer and information security procedures on a routine basis to the practice team.
- Ensure all practice security procedures are being followed and foster a security culture within the team.
- Communicate relevant updates, changes and/or legislative requirements at team meetings and document these discussions in the minutes.
- Educate new team members on the contents of this policy and provide it as part of the induction process.
- Record the education given to individual team members in the staff training log. Education should include:
    - Computer rights and responsibilities.
    - Network access and use.
    - Acceptable online practices when using email, social media, internet, work computers and devices.
    - Maintaining good passwords.
    - Reporting suspicious online activity.
- Maintain the practice's My Health Record Policy and review it annually.
- Ensure all staff are informed of the My Health Record Policy.
- Ensure all staff requiring access to the My Health Record system undergo the required training.
- Update the practice's website as required.

External IT support provider

Our practice has a regular external IT support provider who is responsible for the maintenance and repair of our computer hardware and software systems.

Our external IT support provider is: Medical IT

Our external IT support provider will provide a written Service Level Agreement which includes details and procedures as follows:

- Privacy and confidentiality.
- Managing and updating virus/spam protection software.
- Disaster recovery procedure.
- Ownership of intellectual property.
- Remote access.
- Backup and restoration procedures.
- Time period for regular updates of programs.
- Maintenance schedules.
- Response times.
- Costs – routine, additional, after-hours.
- Audit logs.
- Secure disposal of information assets.
- Cloud services.
- Roles and responsibilities of the external IT support provider and the duties required of the practice's computer security coordinator.
- Regular assessment of practice threats, vulnerabilities, and controls assessments.
- Reporting and acting on any data breaches.

A review of the external IT support provider and Service Level Agreement will be conducted on a yearly basis.

A signed confidentiality agreement is in place with the external IT support provider, along with individual employees of the provider who access the practice's computer systems.

Responsibility-based access

All practice staff will be given responsibility-based access to electronic systems determined by their roles and functionality required as follows:

- **Systems administrator:** this level of access is the highest and is only granted to IT/security trained external service providers for maintaining the server, operating system network functions and software support. All installation/upgrades of programs are to be conducted by the external IT support provider. Remote access will be granted.
- **Computer security coordinator, practice manager and principal/s:** this access includes administrative functionality on the financial, clinical and network systems. Remote access will be granted.
- **Receptionists:** this level of access is for patient administration such as appointments and billing. There is no access to clinical programs. Remote access will not be granted.
- **Clinical practice team members:** this level of access is for use of the clinical programs. This access level may be further subdivided where delineation between the doctor, nursing and allied healthcare staff access is required. Remote access may be granted to work remotely or perform after-hours duties.
- **Guest clinical account:** this level of access is for locums and agency nurses. Access is given to clinical records as required to perform duties, but no access to practice financials are available. This access level may be further subdivided where delineation between the doctor, nursing and allied healthcare staff access is required. Remote access may be granted to work remotely or perform after-hours duties.
- **Other staff (researchers, students, software vendors and other healthcare provider organisations):** This level of access will vary depending on the activities the person is undertaking. Generally, remote access will not be granted.

Password maintenance

All practice staff will have unique identification for all protected systems. Access will be by individual password only, which will be changed every 120 days or immediately if compromised.

- Passwords must not be generic (e.g. each staff member will have their own account).
- Passwords must be private and not shared.
- Passwords must not be reused.
- Passwords must be made up of 6 to 8 characters with alpha, numeric and special characters.
- Passwords must not use:
  - dates of birth
  - family or pet names
  - dictionary words.
- Passwords must not be written on pieces of paper or stored in a word document.
- Staff must select ‘no’ when a computer offers to automatically remember a password for websites.
- Staff must enable multi-factor authentication (MFA) wherever possible.
- Staff must keep their passwords private and not divulge them to anyone.

Password management

- Only the computer security coordinator or system administrator can reset passwords.
- User identifications are archived and removed when staff terminate employment at the practice.
- A lock-out will occur after three unsuccessful login attempts to an account.
- Passwords are stored in the following password management program:

Screen confidentiality

- Computer screens with confidential information must be out of view of security cameras and patients.
- Automatic session time-outs must be utilised to prevent unauthorised computer access when unattended.
- Clinical staff must exit the previous patient’s electronic file before the next patient enters the room.

Privacy policy and confidentiality agreement

Our practice has a privacy policy that complies with the Australian Privacy Principals and covers:

- practice procedures
- staff responsibilities
- patient consent
- access and collection of information.

All staff must sign the practice's confidentiality agreement on commencement of employment. This document is stored in the individual staff member's personnel file.

Backup

Backup is the process of copying files and databases so they are preserved in the event of equipment failure or other catastrophes.

Backup – frequency and access

- Our practice's external IT support provider conducts an offsite backup of the server, files, databases and software, which is written into the Service Level Agreement.
- Our practice has an automatic system for the backup of the server, files, databases and software, which is stored on network attached storage & cloud storage (Servers are located in Australia).
- Only the Medical IT have access to the backups.
- Backups are conducted automatically. Onsite backups twice daily. Offsite backup once daily.
- All backups are encrypted and password protected.

Our practice operates a backup log that documents each backup, which is located, on the server and in the cloud.

\

Backup – reliability and data restoration procedure

Our backup systems are routinely checked by Medical IT for reliability and the outcome is tracked as outlined below:

Restored are done and checked on a quarterly basis.

When we need to restore information on computer systems due to a server failure, the procedure is as follows:

- Contact Medical IT
- Locate restore point.
- Ensure that all other computers have logged out of the server.
- Restore Point or Perform restore for particular system/files.

- Check that the system/files restored look correct (name, size and date).
- Check that the system functions correctly.

Backup – data testing procedure

Our practice tests the backup system quarterly and when system changes are made.

The procedure is as follows:
- Restore file/system on a different computer to the one on which the system normally runs.
- Check that the restored system functions correctly.
- Compare the records to ensure that the restored files contain the latest information.

Anti-malware/antivirus software

Anti-malware, also known as antivirus software, is a computer software program that protects computers against malware and cybercriminals. The software searches for known threats and monitors the behaviour of all programs, flagging suspicious activities by preventing, detecting and removing malware.

Our practice's anti-malware/antivirus software is: Windows Defender with Datto EDR (Endpoint Detection and Response)

- Our practice has anti-malware installed on all computers and laptops
- Automatic updating of anti-malware software is enabled on all computers/servers.
- Automatic scans of computers are enabled.
- Staff are trained to be vigilant of suspicious emails, etc. and are educated to:
  - not respond or click on links in emails from unknown sources
  - only open attachments where the source of the files is known
  - ensure all files downloaded from the internet are scanned for viruses
  - report suspicious pop-up messages
  - report unusual activity on the system.
- In the event of a malware incident, the computer security coordinator will:
  - call the practice's external IT support provider for assistance
  - disconnect internet (and email) connections
  - virus scan all computers
  - isolate infected computers (disconnect from the network)
  - review virus update procedures.

In our practice, cookies are turned off in web browsers. There are exceptions whereby some legitimate software may need this to function properly.

Firewall

A firewall is a security software that prevents unauthorised (and usually external) access to information stored on a private network and controls the flow of data according to specific rules defined by the practice.

Our practice has DrayTek firewall installed as the internet modem. Testing of this firewall is conducted by the external IT support provider or computer security coordinator on request.

Cybersecurity incident response

Our practice has installed threat prevention and email filtering software to detect and mitigate malware, network-based attacks and online scams.

Staff members are trained to recognise and report breaches as soon as they occur so that the practice can quickly respond to the situation. Unusual activities may include the following:

- Accounts and network not being accessible.
- Passwords no longer working.
- Data is missing or altered.
- Hard drive running out of space.
- Computer keeps crashing.
- External stakeholders receiving spam from the practice's email account.
- Receiving numerous pop-up ads.

Data breaches can be through various means:

- Hacking, meaning there has been unauthorised access to or control over computer network systems for some illicit purpose.
- Loss of an electronic storage device (or paper records containing personal information).
- Employees accessing personal information outside the scope of their employment.
- When sending a patient's personal details and/or health information to the wrong recipient.
- Being deceived into improperly releasing the information of another person.
- Accidental or inadvertent disclosure.

Our practice operates an access management system to determine if internal staff have entered or altered data. Each data breach will be assessed on a case-by-case basis based on the guidelines and recommendations outlined by the OAIC Data Breach Preparation and Response documentation.

In the event that a breach has been detected via the computer system, the computer security coordinator will contact our external IT support provider who will implement the following procedure:

- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off computers to stop the threat from spreading.
- Determine the source of the incident, identifying the fault, repairing and restoring systems to business as usual. This includes checking on the anti-malware software and applying the latest patches to diminish the likelihood of cyber-attacks.
- Evaluate the incident before and after and determine any ongoing additions or modifications that need to be made to the system. Update the Computer Information Security Policy and Procedures with these changes.
- Determine if the breach is classified as an 'eligible data breach'.

If the data was leaked intentionally or accidentally by an employee:

- Modify access privileges.
- Reset passwords.

When data is determined to be intentionally leaked by an employee, the employee will be subject to corrective action, including verbal warnings, formal reprimands, possible termination of employment and legal action if appropriate. Each issue will be dealt with on a case-by-case basis and any consequences will be commensurate with the violation.

The computer security coordinator will confer with the external IT support provider to estimate the time for repair and to confirm when the breach has been secured. In the interim, the practice will implement manual methods or use backup workstations and devices.

The external IT support provider will document any evidence and consider if it is appropriate to report the incident to the Australian Cybercrime Online Reporting Network.

A log is maintained for all faults and breaches, detailing the following information:
- The date of the fault.
- Who logged the fault.
- When the fault was discovered.
- How the fault was rectified.
- If the fault was reported to an official body.

Notifiable data breach response and reporting

Our practice uses the OAIC Data Breach Preparation and Response documentation for guidance on handling notifiable data breach situations. Each data breach will be assessed on a case-by-case basis.

A notifiable eligible data breach occurs when the following criteria are met:
- There is unauthorised access to or disclosure of personal information held by the practice (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- It is likely to result in serious harm to any of the individuals to whom the information relates. When assessing whether serious harm is likely, the practice will consider the following factors:
    - Whose personal information, such as young persons and vulnerable individuals, may be at risk?
    - How many individuals were involved?
    - Is the personal information encrypted or otherwise not easily accessible?
    - What parties have gained, or may gain access to, the personal information?
- The practice has been unable to prevent the likely risk of serious harm with remedial action.

In the event that a breach has been detected via the computer system, the computer security coordinator will confer with our external IT support provider who will implement the following:
- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off computers to stop the threat from spreading.
- Eliminate the problem with the removal of the threat.
- Recover from the incident by repairing and restoring systems to business as usual, including checking on the anti-malware software and applying the latest patches to diminish the likelihood of cyber-attacks.
- Identify if any systems and processes need improving and make those changes.
- Evaluate the incident before and after and determine any ongoing additions or modification that need to be made to the system.
- All data breaches will comply with the procedures and guidelines outlined in the OAIC Data Breach Preparation and Response documentation and tracked in the Incidents and Actions Register.

After consultation with the principal and medical defence organisation, the computer security coordinator will determine if the breach is an eligible data breach and needs to comply with the mandatory notification law.

If it is determined that an eligible breach has occurred, the mandatory notification process is as follows:
- Report, as soon as practicable, to the Office of the Australian Information Commissioner detailing the breach on the Notifiable Data Breach Form.
- Subsequently notify:
    - Option 1 – all individuals whose personal information was part of the data breach.
    - Option 2 – only those individuals at risk of serious harm.
- If neither Option 1 or 2 are practicable:
    - Option 3 – a notification of the data breach will be published on the practice's website.

Notification can be conducted using the following methods, dependent on the circumstances:
- Person-to-person conversation.
- Telephone call.
- SMS.
- Mail.
- Social media post.
- Practice website.

Power failure and IT systems

In the event of a loss of power to the premises, the clinical system server is protected by an uninterruptible power supply (UPS) if applicable. This provides power for a short amount of time during which the server can be closed down and switched off without the risk of data corruption. The UPS only provides power for a limited period of time (battery life is approximately 15-20 minutes).

Urgent tasks that require web access will be conducted through the practice's mobile phone.

During a mains electrical failure, computers will be switched off to protect them from a power surge when the power is restored.

In the event of a full power outage, the practice will utilise the practice's laptop computer on battery power and call up the appointments list of the daily appointment backup.

The following senior staff members have access to the practice software at home:

IT system crashes, system errors and loss of data

In the event of the IT system being rendered unusable (e.g. hard drive crash or malicious virus), report the situation to the external IT support provider and request a timeframe for reuse of the system.

Assess the impact of the situation and determine the next steps from the list below:

- Inform patients currently in the practice about the situation.
- Print out appointment lists from the most recent appointment backup, with priority given to patients already in the practice and patients with appointments within the next 30 minutes.
- Advise patients wanting to make an appointment to call back if it is not urgent (timeframe will be dependent on advice from the external IT support provider).
- During consultations, medical staff need to utilise the individual GP's emergency box and utilise the blank paper notes and include the patients name, address and date of birth. Medical staff are responsible for entering their own data once the system is operational.
- Prescription pads are kept in each GP's emergency box. All prescriptions must be entered into the patient file once the system is operational.
- Practice letter heads are kept in the GP's emergency box for urgent referral letters. All letters must be entered into the patient file once the system is operational. A formal letter will also be forwarded to the specialist/allied health provider.
- Reception staff are to record all urgent enquiries on the message pads provided in the emergency box located in reception. Details taken must include the patient's name, date of birth, address, telephone number and GP's name. All messages must be dated, and time of message recorded before passing on to the relevant person.
- Utilise paper Medicare forms and handwrite manual invoices/receipts.

Theft of IT equipment

In the case of IT equipment theft, report the situation to the external IT support provider and request a timeframe for the replacement of equipment and restoration of the system.

Passwords for all staff must be changed if any IT equipment is stolen.

Risk analysis

A risk analysis for managing computer information security is conducted at least yearly and is categorised into the following three areas:

- Human (unintentional or deliberate, e.g. theft of a laptop containing clinical or business information, inadvertent viewing of a patient's information by non-practice staff or another patient).
- Technical (e.g. a hard drive crash or data corruption from a virus).
- Environmental (e.g. a natural disaster such as fire, flood, earthquake, storm or cyclone).

Potential risks and threats to be considered in the risk assessment:

- Errors and omissions (e.g. accidental file deletion, inability to restore data from backups).
- Unintentional access of information systems by practice staff.
- Unintentional viewing of information systems by non-practice staff.
- Unauthorised system or network access.
- Non-compliance with legislative requirements.
- Theft or damage of equipment.
- Inappropriate disclosure or theft of information.
- Employee sabotage.
- Fraud.
- Email threats (e.g. phishing, spamming or corrupted attachments).
- Deliberate misuse of information systems.
- Malicious software.
- Software/hardware failure.
- Power disruptions.
- Physical protection of data that is stored offsite (e.g. data storage devices such as hard drives).

Our practice utilises a Business Risk Management System to aid in identifying risks, assessing the risks and putting in place strategies to mitigate the risks.

(If you require assistance, refer to the RACGP Computer and information security templates 2.24: Risk assessment – threat vulnerability and controls, pages 26 to 35.)

Secure messaging systems (SMS)

In our practice, the use of general email to send any health information to a patient, health professional or organisation is discouraged. Secure message delivery is the preferred method of transmission.

Secure message delivery involves two processes: encryption and authentication. Encryption means that the data is electronically 'scrambled' so that it cannot be read unless the information is decrypted. Authentication means that the sender can be verified, which is done by using electronic signatures.

To use secure message delivery, both the sending and receiving parties must use compatible encryption processes. The practice utilises secure electronic communication/messaging systems for clinical documents, patient/healthcare specific information and information that contains sensitive business information.

The secure messaging systems used by the practice include: Best practice software internal messaging system, WhatsApp application, practice emails

There are exceptions to the requirement of utilising secure message delivery, such as putting a patient or healthcare professional at risk, or where the recipient is unable to receive secure messages. In these circumstances, approval must be gained from the treating GP and authorised by the practice principal.

Our practice receives pathology, radiology, discharge summaries and specialists' letters via the secure messaging system.

Encrypted emails

Our practice does not use encrypted email and cannot guarantee confidentiality of information sent by email. As a result, email communication containing patient details is discouraged.

Electronic asset register

Our practice has an electronic asset register located in dropbox and in reception CISS folder

Our electronic asset register lists assets in two categories:

- Hardware (e.g. computers, communications equipment, mobile devices, smart phones, tablet devices, medical equipment that interfaces with the computer systems, backup media and uninterruptible power supplies).
- Software (e.g. application programs, operating system/s, communications programs, clinical and practice management programs, email, firewall, backup and anti-malware programs.)

My Health Record policy

Our practice maintains a My Health Record policy, which is reviewed annually.

- All staff are informed of the My Health Record policy.
- All staff required to use the My Health Record system will undergo training before accessing the system. Our practice utilises the Australian Digital Health Agency Recommended Training Checklist and Declaration. Signed copies of this document are kept in the individual's personnel file.