Privacy Policy

Table of Contents

The Practice Website

Policy

In complying with the *Privacy Amendment (Private Sector) Act 2000*, our practice provides the following advice to users of our website about the collection, use and disclosure of personal information.

The aim of this advice is to inform users of this site about:

What personal information is being collected?

Who is collecting personal information?

How personal information is being used?

Access to personal information collected on this site

Security of personal information collected on this site.

The practice privacy policy is posted on the website and available for download.

The website is continually monitored to ensure it is kept current and up to date. It contains the minimum information required on the practice information sheet. Refer Section 5 Practice information sheet. Any changes to the practice information sheet are also reflected on the website.

If it contains any advertising the practice should include a disclaimer that the practice does not endorse any advertised services or products. Advertising must comply with the MBA Code of Conduct on advertising available at: **Good Medicine Practice**

Internet and Email Usage

Policy

All staff within the practice are to assist in mitigating security risks. This includes being aware of the risks associated with email and internet usage.

All staff are to use the internet, email and secure messaging in a manner which meet our privacy obligations and are to use such resources in a respectful and professional manner.

Procedure

To avoid unnecessary risk to information systems, the following applies:

Internet usage

- internet use is for business, clinical and research purposes only
- all downloads accessed from the internet must be scanned for viruses

- all sites accessed must comply with legal and ethical standards
- web browser security settings are not to be changed without authorisation

Staff members are encouraged to use the Internet for research activities pertaining to their role, however, should be aware that usage statistics are recorded and submitted to Management as required.

Staff members have full accountability for Internet sites accessed on their workstations, and are expected to utilise this tool in an acceptable manner.

This includes (but is not limited to):

- limiting personal use of the Internet
- accessing ONLY reputable sites and subject matter
- verifying any information taken off the Internet for business purposes prior to use
- not downloading any unnecessary or suspect information
- being aware of any potential security risks - i.e. access / viruses
- not disclosing any confidential information via the Internet without prior permission from the practice manager - i.e. Credit Card number
- maintaining the Practices confidentiality and business ethics in any dealings across the Internet
- observing copyright restrictions relating to material accessed/downloaded.

The Practice reserves the right to check individuals Internet history as a precaution to fraud, viruses, workplace harassment or breaches of confidence by employees. Inappropriate use of the Internet facility will be fully investigated and may be grounds for dismissal.

This practice uses antivirus, anti-malware and anti-spyware which are centrally installed and managed and locally deployed.

Email usage

Communication with patients via electronic means (e.g. email) is conducted with appropriate regard to the privacy and confidentiality of the patient's health information.

Our practice uses the following confidentiality and privilege notice on outgoing emails that are affiliated with the practice:

‘This message is confidential and should only be used by the intended addressee. If you were sent this email by mistake, please inform us by reply email and then destroy this message. The contents of this email are the opinions of the author and do not necessarily represent the views of the Practice."

Best practice when using email:

- Do not open unexpected email even from people known to you as this might have been spread by a virus.
- Use an antivirus mail filter to screen email before downloading.
- Do not use the ‘preview pane’ in your email program as this automatically opens your email when you click on the header.
- Save attachments and check for viruses before opening or executing them (note this does not relate to the clinical secure messaging but to attachments received through email and websites).

- Do not run programs directly from websites. If files are downloaded, check for viruses first.
- Email use that breaches ethical behaviours and/or violates copyright is prohibited.
- Do not send or forward unsolicited email messages, including the sending of ‘junk mail’ or other advertising material (email spam).
- Do not use email for broadcast messages on personal, political or non-business matters.
- Practice staff are never to send emails that might be construed as offensive or constitute as any form of harassment.

Emails and internet usage will be monitored by the Practice Manager including discretion to blacklist certain sites such as personal email or social media sites.

All staff have signed a computer use agreement as a condition of their employment.

Useful Resources:

[RACGP Social Media Guide]

[Recognise scam or hoax emails and websites]

[Australian Privacy Principles]

The Privacy Act and Australian Privacy Principles

Policy

“Sensitive information” is covered by the APPs. This information includes:

- Medical information
- Personal details including contact details, Medicare number
- Biological samples
- Radiology results (x-rays)

Review APPs and check practice for compliance

1. Have a procedure for handing privacy inquiries and complaints
2. Designate a staff member responsible for receiving and responding to complaints
3. Determine how to manage a patient who wishes to interact with the practice anonymously
4. Determine a staff member responsible for decision on dealing with unsolicited personal information (APP4)
5. To comply with APP7, have a system for tracking patients who do not want the practice contacting them about practice services (ie opt out).
6. If personal information may be sent overseas check details of the cloud service provider. (APP8)
7. Do not use a government related identifier – eg Medicare number, drivers licence number, passport number and Centrelink reference number. (APP9)
8. Ensure patient details are accurate – incorporate this check into the patient identification process. (APP10)

9. Protection of information from "interference" may be addressed by use of passwords by staff to access the practice's medical records system, and changing the passwords on a regular basis. (APP11)
10. Have a procedure and a designated staff member to facilitate consideration of patient access to medical records, ensuring responses are within the required, "reasonable period" which is no more than 30 calendar days; ensure that fees are not "excessive" (consider use of the AMA suggested fees) (APP12); and to facilitate management of correction of information.

Privacy and Confidentiality

Policy

This is an extremely important code of ethical behaviour and must be maintained at all times by all staff.

The legal requirements of confidentiality extends from the Practice Principal/s to all Clinicians and staff.

VERBAL BREACH of confidence - Discussion of patient's conditions with staff members, families, friends and others.

VISUAL BREACH of confidence - Leaving patient's records in full view of any other party.

AUDITORY BREACH of confidence - Discussing patient matters (in hearing range of other's nearby).

The Privacy Act

The Privacy Amendment (Sector) Act 2000 extends the operation of the Privacy Act 1988 to cover the private health sector throughout Australia.

The Privacy Act requires our practice to abide by the 13 Australian Privacy Principles (APPs):

1. APP 1 – open and transparent management of personal information
2. APP 2 – anonymity and pseudonymity
3. APP 3 – collection of solicited personal information
4. APP 4 – dealing with unsolicited personal information
5. APP 5 – notification of the collection of personal information
6. APP 6 – use and disclosure of personal information
7. APP 7 – direct marketing
8. APP 8 – cross-border disclosures
9. APP 9 – adoption, use or disclosure of government related identifiers
10. APP 10 – quality of personal information
11. APP 11 – security of personal information
12. APP 12 – access to personal information
13. APP 13 – correction of personal information

Resources:

Information regarding complying with the legislation is available at the Office of the Australian Information Commissioner

The RACGP's Privacy and managing health information in general practice at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy

Privacy Policies for GPs (OAIC August 2015)

Privacy Policy - Notifiable Data Breach Scheme

Policy

The practice recognises that prevention of data breaches is much better than dealing with them after the fact. This policy also supports the practice's other obligations under the Privacy Act.

Organisations covered by the Privacy Act have obligations under the Act to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

A data breach is:

- Unauthorised access to or unauthorised disclosure of personal information, or
- Lost personal information and likely unauthorised access or disclosure

Examples of a data breach include an email sent to the wrong person, a lost laptop containing patient information or your database being hacked.

If a breach has occurred, the practice will consider if the breach is likely to result in serious harm to an individual.

For 'serious harm', consider:

- Type of information and sensitivity
- Protections in place to prevent disclosure
- Persons who have obtained or could obtain data
- Nature of harm and number of people affected

'Serious harm' can be:

- Psychological
- Emotional
- Physical
- Reputational
- Financial

The practice has a **data breach response plan** that helps establish robust and effective procedures in the event of a data breach. The purpose of the plan is to ensure that quick actions can be taken after discovering a data breach.

A data breach response plan is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by the practice in managing a breach if one occurs. This includes:

- the members of the data breach response team (response team)
- the actions to be taken if a breach is suspected, discovered or reported by a staff member or other person, including when it is to be escalated to the response team
- the actions the response team is expected to take.

The plan clearly identifies those actions that are legislative or contractual requirements.

The purpose of a response team is to ensure that the relevant staff, roles and responsibilities are identified and documented before the data breach happens.

All staff is aware of the plan, response team members and clearly understands what needs to happen in the event of a data breach.

The plan is regularly reviewed and tested including simulating the practice's response to a hypothetical data breach

Procedure

The practice has a data breach response team. The data breach response team consists of:

- Practice principal/s - Dr Suresh Kesavan
- Practice manager - Mark Dellow
- Practice's IT service provider
- Insurance/ Legal - Avant Mutual Group Limited

All members of the practice team are aware of the actions to be taken if a breach is suspected, discovered or reported by any staff member.

The data breach response team is informed of ***any*** potential breaches. The team should be informed as soon as a breach or potential breach is identified. The team should be informed verbally if a team member is available, or via email if the team members are not on site.

In the event of a breach, the response team will gather and document all available details about the nature of the breach, including any technological aspects of the breach, timing, duration and format. This might include:

- details of person/organisation reporting the potential breach ;
- what action they claim to have taken in response to the situation (e.g. email or fax received by mistake; discovery of sensitive information online etc.);
- forensic analysis of data access or information transfer in the event of unauthorised database/system access; analysing CCTV footage, possibly contacting relevant police or security services.

Once this process has been undertaken or commenced, the practice could contact the practitioners'/practice's medical defence organisation for advice and notification.

The response team will:

- assess if the breach is likely to result in serious harm to an individual/individuals with assessment to occur as soon as possible and within 30 days.
- where possible, undertake remedial action to prevent the likelihood of serious harm
- depending on the size and nature of the data breach, decide the most appropriate form of contacting affected individuals, or individuals potentially affected by the breach (e.g. individual phone calls, emails, written letter, newspaper advertisement, signage in the practice etc.)
- contacts the individuals at risk of harm and Office of the Australian Information Commissioner (OAIC) as soon as practicable, if it is not possible to take remedial action

The response team will also consider:

1. If the breach or suspected breach indicate a systemic problem with the practice's or procedures.
2. Strategies to identify and address any weaknesses in data handling that contributed to the breach
3. Other issues relevant to the practice's circumstances, such as the value of the data to the practice or issues of reputational risk
4. A system for a post-breach review and assessment of the practice's response to the data breach and the effectiveness of the data breach response plan.

The data breach response plan is reviewed on a 6 monthly basis.

Additional Information about the Notifiable Data Breach Scheme

From 22 February 2018, organisations covered by the Privacy Act 1988 are required to notify individuals likely to be at risk from serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner (OAIC).

Helpful resources:

Privacy basics and data breaches (Avant 08/11/2017)

New privacy laws coming into force – are you ready? (Avant 23/10/2017)

Guide to developing a data breach response plan (OAIC April 2016)

Notifiable Data Breach Scheme Decision Making Flowchart (Avant October 2017)

RACGP Computer and Information Security Standards Data incident/breach report

Notifying individuals about an eligible data breach (OAIC December 2017)

Preventing data breaches (Avant 01/02/2018)

OAIC Data breach notification guide: A guide to handling personal information security breaches

Security and Privacy of Records

Policy

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

Health records must be kept where constant staff supervision is easily provided. Personal health information must be kept out of view and must not be accessible by the public.

All patient health information must be considered private and confidential, and therefore must not be disclosed to family, friends, staff or others without the patient's consent. This information includes medical details, family information, address, employment and other demographic and accounts data obtained via reception.

Any information given to unauthorised personnel will result in disciplinary action, possible dismissal and other legal consequences. Each staff member must sign a confidentiality agreement on commencement of employment.

In addition to Federal legislation, our practice also complies with State or Territory legislation. Care must be taken that individuals cannot see computer screens showing information about other individuals. Screensavers or other methods of protecting information must be engaged.

Access to computerised patient information is be strictly controlled with personal logins and passwords. Staff must not disclose passwords to unauthorised persons. Screens need to be left cleared when information is not being used. Terminals must also be logged off when the computer is left unattended for a significant period of time. Items for the pathology couriers or other pick ups must not be left in public view.

When not in attendance, staff must ensure that prescription pads, prescription computer generated paper, letterhead, scripts, medications, health records and related patient information are out of view. They must also be stored in areas only accessible to authorised persons.

Facsimile, printers and other electronic communication devices must only be accessible to authorised staff.

Procedure

In our practice

- computer screens are positioned so that individuals cannot see information about other individuals
- access to computerised patient information is strictly controlled with passwords and personal logins
- automatic screen savers
- computer terminals are logged off when the computer is left unattended for a significant period of time.

In our practice, prescription pads, prescription computer generated paper, letterhead, scripts, medications, health records and related patient information are stored in locked store cupboard in the staff rooms.

In our practice, the facsimile, printers and other electronic communication devices are located within consult rooms and behind reception desk.

In our practice, items for pathology couriers or other pickups are left in a secure location.

Accessing to and Sharing of Patient Information

Policy

In our practice

- computer screens are positioned so that individuals cannot see information about other individuals
- access to computerised patient information is strictly controlled with passwords and personal logins
- automatic screen savers
- computer terminals are logged off when the computer is left unattended for a significant period.

In our practice, prescription pads, prescription computer generated paper, letterhead, scripts, medications, health records and related patient information are stored in locked store cupboard in the staff rooms.

In our practice, the facsimile, printers and other electronic communication devices are located within consult rooms and behind reception desk.

In our practice, items for pathology couriers or other pickups are left in a secure location.

Request for Personal Health Information

Policy

Patients of our practice have the right to access their personal health information under privacy information. Our practice informs patients that they are able to access their health information. This is done via the practice information sheet, notice in the waiting area and on the practice website (if applicable).

On request for access to personal health information, our practice documents each request and endeavours to assist patients in granting access where possible and according to the privacy legislation. Exemptions to access must be noted and each patient or legally nominated representative must have their identification checked prior to access being granted.

Our practice has a designated person – Dr Suresh Kesavan with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security policy

Procedure

Computerised Records

Our practice is considered paperless and has systems in place to protect the privacy, security, quality and integrity of the personal health information held electronically. Appropriate staff members are trained in computer security policies and procedures.

Our practice follows this procedure on request for access to personal health information in accordance with privacy legislation:

1. Document the patient's request (on patient chart and via written request form) and forward a request to the patient's GP to check for exemptions
2. Check the patient's or legally nominated representative's identification prior to access being granted.
3. Provide personal health information within reasonable period of time as outlined in the Privacy legislation.

Helpful Resource

Office of the Australian Information Commissioner

AMA Ethical Guidelines for Doctors on Disclosing Medical Records to Third Parties 2010. Revised 2015

Computer Securtiy

Policy

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held. Appropriate staff is also trained in computer security policies and procedures.

A staff member – Dr Suresh Kesavan has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

The RACGP Handbook for the Management of Health Information in Private Medical Practice and Information security in general practice provide information and explanations on the safeguards and procedures that need to be followed by general practices in order to meet appropriate legal and ethical standards concerning privacy and security of patient health information. These documents also contain suggestions for additional security procedures.

Our practice has the following areas documented in the computer security policy:

- Practitioners and staff have personal passwords to authorise appropriate levels of access to health information
- screensavers or other automated privacy protection devices are enabled
- backups of electronic information are performed at a frequency consistent with a documented information disaster recovery plan
- backups of electronic information are stored in a secure offsite environment
- backups are tested
- antivirus software is installed and updated
- all internet connected computers have hardware/software firewalls installed
- disaster recovery plan that has been developed, tested and documented
- data transmission of patient information over a public network is encrypted.

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

- current equipment register documenting hardware and software specifications and locations, network information, technical support
- logbooks/print-outs of maintenance, backup including test restoration, faults, virus scans
- folder with warranties, invoices/receipts, maintenance agreements.

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.

Procedure

In our practice, the staff member responsible for coordinating IT security is the Practice Manager.

This staff member is responsible for the following activities:

- overseeing the development of documented IT security policies and procedures
- overseeing the development of a computer disaster recovery plan
- ensuring that there are test runs of disaster recovery procedures at specified intervals
- ensuring revision of the disaster recovery plan at specified intervals
- keeping an IT assets register (hardware, software, manuals and technical support)
- ensuring that there is an access control policy in place
- ensuring that staff are aware of maintaining password security
- ensuring that screensavers are in place
- establishing a routine back-up procedure
- ensuring that restoration of data is tested at specified intervals
- ensuring that anti-viral software is installed on all computers and the virus definitions are updated daily
- ensuring that technical advice is sought and acted upon for the installation of appropriate firewalls
- ensuring that computers, especially the server, are adequately maintained
- ensuring that the computer system can deal with fluctuations in the power supply

- investigating the appropriate means of encrypting confidential information prior to electronic transfer
- coordinating the application, use and storage of digital certificates
- ensuring our practice understands encryption
- arranging computer security training for members of our practice.

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

- paper prescription pads/sick certificates etc.
- appointment schedule printout and manual book.
- consultation notes.
- emergency numbers.

Useful Resources:

Steps to protect your practice from a cyber security incident: things to consider (Avant, July 2019)

Responding to a cyber security incident (Avant, July 2019

Cyber security checklist (Avant, July 2019)

RACGP Computer Security Guidelines

eHealth

Information Security (inc. MyHealth Record)

Policy

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held. All staff are educated and regularly trained in our computer security policies and procedures. Our policies and procedures are a source of information to clarify roles and responsibilities, and to facilitate the orientation of new practice team members.

The RACGP Computer and Information Security Standards provide information and explanations on the safeguards and procedures that need to be followed by general practices in order to meet appropriate legal and ethical standards concerning privacy and security of patient health information. These documents also contain suggestions for additional security procedures.

Our practice has a *My Health Records* policy that covers the specific requirements of *My Health Records Act 2012* and *My Health Records Rule 2016*

Our practice has the following information to support the computer and information security policies and procedures:

- current asset register documenting hardware and software specifications and locations, network information, technical support
- logbooks/print-outs of maintenance, backup including test restoration, faults, virus scans

- folder with warranties, invoices/receipts, maintenance agreements.

Procedure

Practice Team Agreements

Upon employment, every practice team member is given confidentiality and privacy agreements to sign, together with an appropriate computer use agreement. These act to protect the owners of the practice in the event of legal action against the practice arising out of a security breach.

These agreements are used to ensure that practice team members and other people working in a practice who may have access to confidential patient or business information comply with privacy and security of information as required under legislation, including the *Privacy Act 1988* and the Australian Privacy Principles.

External Service Provider Agreements

Unique contractual arrangements are made with all external service providers including information in relation to:

- data confidentiality
- remote access
- backups and restoration procedures
- response times
- costs
- regular maintenance
- audit logs
- secure disposal of information assets
- cloud services

My *Health Records* Policy

The following information is taken from *My Health Records Rule 2016:*

The Practice will enforce the following in relation to all its employees and any Organisation with whom we engage under an agreement/contract:

- The manner by which the Practice authorises persons accessing the *My Health Records* system via or on behalf of the practice
- The manner of suspending and deactivating the user account of any authorised person:- who leaves the practice,
- The manner of suspending and deactivating the user account of any authorised person whose duties no longer require them to access the *My Health Records* system,
- The manner of suspending and deactivating the user account of any authorised person whose security has been compromised.

Our practice ensures the following:

- Training will be provided before a person is authorised to access the *My Health Records* system, including in relation to how to use the *My Health Records* system accurately and responsibly, the legal obligations on the practice and our staff members using the *My Health Records* system and the consequences of breaching those obligations.

- The process for identifying a person who requests access to a patient's *My Health Records* is clear and followed and the person's identity is communicated to the System Operator so that the healthcare provider and the practice is able to meet its obligations.
- Physical and information security measures are established and adhered to by the healthcare provider, the practice and people accessing the *My Health Records* system via or on behalf of the healthcare provider, the practice, including that user account management measures are implemented.
- Mitigation strategies to ensure *My Health Records* related security risks can be promptly identified, acted upon and reported to the Practice Manager.

The Practice will authorise the staff members within its team that require access to the *My Health Records* system by:

- Generating and maintaining an authorised employee register, which includes the name and HPI-I for all health care professionals working at the Practice or on behalf of the practice.
- Registering both our HPI-O and the HPI-Is of our practitioners for publication in the Healthcare Provider Directory (HPD)
- Recording and keeping current the credentials of all our staff who require access to the *My Health Records* system

For a staff member who leaves the Practice we will deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.

For a staff member whose duties no longer require them to access the *My Health Records* system we will deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.

For a staff member whose security has been compromised we will immediately deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.
- Keeping record of the details surrounding the event (e.g. who and why).
- Pursuing the necessary disciplinary action if necessary

Training will also be conducted as new functionality is introduced into the system. We will utilise the training resources made available by the System Operator, as a minimum. To assist in ensuring training completion and audit purposes, a record is kept confirming the training completed by each authorised staff member and the date completed.

Notwithstanding any action the System Operator may take with regard to data breaches, the practice will continue to implement local staff conduct and disciplinary policies with regard to any staff unauthorised access to the *My Health Records* system.

Our practice will also ensure the following:

- staff members that we authorise to access the system can be identified by either a unique local identifier or system log-in
- the Practice has current and adequate IT system anti-viral software
- our Disaster Recovery Plans are current and executable
- ensure our IT systems and hardware is physically protection against unauthorised access or hacking
- that each authorised user of the system has a secure password

We regularly review our security and procedures for accessing the *My Health Records* system, report the findings to management and revise our procedures accordingly.

The practice has set out a risk reporting procedure to allow staff to inform management regarding any suspected security issue or breach of the system.

All staff in the practice and any healthcare providers to whom the organisation supplies services under contract have access to this Policy. The practice will notify all personnel of changes to these Policies and Procedures when they occur.

Helpful Resources:

Australian Privacy Principles

My Health Record Risk Assessment

Policy

Our practice periodically completes a risk analysis of our information security system and ongoing security needs. This provides assurance of the availability, integrity and confidentiality of all information held within the practice's clinical and business information systems.

Our practice identifies and analyses any threats and vulnerabilities that the practice may be exposed to so the most appropriate security controls can be put in place to minimise these risks. All staff are informed and regularly updated about the risks associated with using computer and information systems.

Procedure

The practice reviews the *My Heath Records* System annually or when any new or changed risks are identified. When performing the review, the following is to be considered:

- potential unauthorised access to the *My Health Records* system using the practice information systems
- potential misuse or unauthorised disclosure of information from a patient's *My Health Records* by persons authorised to access the *My Health Records* system via or on behalf of the practice
- potential accidental disclosure of information contained in a patient's *My Health Records*
- the increasing risks and potential impact of the changing threat landscape (e.g. newer types of security threats such as ransomware)

- the impact of any changes to the *My Health Records* system that may affect the practice
- any relevant legal or regulatory changes that have occurred since the last review.

Records are retained on physical and information assets and every actual or suspected breach in security (accidental or intentional) is to be recorded.

Asset Management

Our practice has an asset register which documents the computer hardware, software and information systems used. The register also records the configuration of the systems that will be used when the disaster recovery plan is invoked. The asset register is updated as each new item is purchased by the practice or new service or application installed. The Computer Security Coordinator is responsible for maintaining the asset register.

The assets are grouped as follows:

- physical assets: computer and communications equipment, mobile devices, smart phones, tablet devices, medical equipment that interfaces with the computer systems, backup media and uninterruptible power supplies.
- software assets: application programs, operating system, communications software. Original software media and manuals are stored securely
- personnel assets: contact details of key members of the practice team and external service providers
- paper documents: contracts, operating and professional guidelines

Threat Analysis

Potential Threats are to be categorised into three areas:

- human (unintentional and deliberate): for example, the theft of a laptop containing clinical or business information, or inadvertent viewing of a patient's information by non-practice staff or another patient
- technical: for example, a hard disk crash or data corruption from a virus
- environmental: for example, a natural disaster such as a bushfire or flood.

Once the potential threats have been identified, the appropriate controls are to be identified. Once the threat has been categorised the following needs to be documented:

- Threat/Risk Source
- Disruption/Impact
- Vulnerability
- Suggested appropriate solutions and mitigation strategies
- Action Required
- Person responsible

Monitoring and Review Planning

Risk management is discussed at practice meetings. Staff are reminded of processes and time is allocated for staff to communicate any concerns/issues. All staff are reminded of their legal responsibilities when interacting with the *My Health Records* system.

Data Breach Response and Recording

Under the *My Health Records Act 2012* a data breach is:

- the unauthorised collection, use or disclosure of health information in an individual's *My Health Records*;
- an event that has, or may have, occurred that compromises, may compromise, has compromised, or may have compromised, the security or integrity of the *My Health Records* system; or
- any circumstances that have or may have arisen (whether or not involving a contravention of the *My Health Records Act 2012*), that compromises, may compromise, have compromised, or may have compromised, the security or integrity of the *My Health Records* system.

In the event of an actual or suspected data breach the following steps are to be followed:

Containment of the breach

- The first step is to contain the breach so that no further damage can be done. Take whatever steps are possible to immediately contain the breach. This may be to isolate the system or disconnect from the internet if this is likely where the breach occurred. If it is not practical to shut down the system (or it might result in a loss of evidence) then suspend user access to the records affected, or suspend a specific user's access.
- Assess whether steps can be taken to mitigate the harm a patient may suffer as a result of a breach.

Initial assessment of the cause of the breach

- The Computer Security Coordinator will lead the initial assessment of the breach. This may need to be done in conjunction with technical support to enable correct evaluation of the cause and be able to make recommendations.
- The analysis will need to consider what personal information the breach involves, what was the cause of the breach, what the extent of the breach is, and what is the potential impact (harm) to individuals of the breach.
- Be mindful of not destroying evidence that may be helpful in determining the cause of the breach or in rectifying the problem.
- Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made using a Data Breach/Incident Report form.

Notification of the breach.

The following need to be notified as soon as possible in the event of a breach or suspected breach:

- Notify the practice management
- Notify the individual effected
- Notify the police if theft or criminal activity is suspected
- Notify the *My Health Records* System Operator
- Notify the OAIC.

For notifications contact:

- the My Health Record System Operator on 1800 723 471; and
- the Australian Information Commissioner on 1300 363 992.

Investigation of the breach

- Ascertain if the information is encrypted or de-identified.
- Identify who is affected by the breach.
- Evaluate what the breach information could be used for.
- Evaluate the risk of harm from the information disclosed by the breach.
- Determine the risk of further breaches of this type.
- Determine if this is a systemic or isolated incident.
- Evaluate what harm could occur to the practice as a result of the breach.

Helpful Resources:

Notification of Data Breaches in the PCEHR System

Guide to handling person information

Australian Privacy Principles

Roles and Responsibilities

Policy

All of the practice team are aware of their roles and responsibilities in regards to computer and information security and receive ongoing training. The specific responsibilities of each role are documented in position descriptions. All staff play a part in the protection of information including recognition of errors or abnormal software behaviour and reporting actual or potential data breaches.

Our practice has a designated Computer Security Coordinator, Responsible Officer and Organisation Maintenance Officer.

Procedure

In our practice, the Computer Security Coordinator is the Practice Manager *(NB: Role can be done by or shared with a Doctor, Senior Receptionist or a Nurse).*

The Computer Security Coordinator is responsible for the following activities:

- overseeing the development of documented IT security policies and procedures
- overseeing the development of a computer disaster recovery plan
- ensuring that there are test runs of disaster recovery procedures at specified intervals
- ensuring all policies and procedures are reviewed at least annually
- maintain an up to date risk assessment including keeping an IT assets register (hardware, software, licences, manuals and technical support)
- ensuring that there is an access control policy in place
- ensuring that staff are aware of maintaining password security
- ensuring clear screen and clear desk policies are followed (e.g. screensavers are activated)
- establishing a routine back-up procedure
- ensuring that restoration of data is tested at specified intervals

- ensuring that anti-viral software is installed on all computers and the virus definitions are updated daily
- ensuring that technical advice is sought and acted upon for the installation of protection systems such as firewalls and intrusion detection
- ensuring that computers, especially the server, are adequately maintained
- ensuring that the computer system can deal with fluctuations in the power supply
- ensuring information transferred electronically is secure (e.g. using secure message delivery)
- coordinating the application, use and storage of digital certificates
- ensuring our practice understands encryption
- Reporting any outstanding security issues and provide updates on security in practice management meetings
- ensuring that the security procedures are being followed and arranging regular computer security training for members of our practice.

In our practice, the Responsible Officer is the Business Owner.

The Responsible Officer (RO) is responsible for the following activities:

- the creation and deactivation of the practice within the Health Identifiers (HI) Service
- the nomination of an Organisation Maintenance Officer (OMO)
- requesting HI Service Operator to process a Change of Ownership for the practice that they represent if necessary
- add/remove links between RO or an OMO with the practice
- update their own demographic details

In our practice, the Organisation Maintenance Officer is the Practice Manager.

The Organisation Maintenance Officer is responsible for the following activities:

- requesting to amend their own demographic details or details of the practice
- administrative access to the practice records that are beneath them in the practice hierarchy and linked to in the HI Service
- add/remove links for other OMOs or healthcare providers that they are responsible for
- Updating the Healthcare Provider Directory for the practice
- provide periodic activity reports to practice management

The Responsible Officer and Organisation Maintenance Officer, as defined in the *Healthcare Identifiers Act 2010* (the HI Act), are to be registered under the Healthcare Identifiers (HI) Service.

Medicare Australia Healthcare Identifiers Service - Initial application to register a Responsible Officer, Organisation Maintenance Officer and a Seed Organisation

Useful Resources:

Australian Privacy Principles

Managing Access

Policy

Our practice monitors authorised access to patient health information and sensitive business information and has different levels of access for different staff member's appropriate to their duties. Our practice practice has a strong password management system to protect the practice against the misuse of information.

Procedure

The positions of staff that are authorised to access patient health information include:

Position of staff member	Program name	Level of access
General Practitioners	Best Practice	All
Front Desk staff	Best Practice	Limited
Nursing staff	Best Practice	All
Practice Manager	Best Practice	All
Practice Principal/s	Best Practice	All

All staff have a position description that clearly outlines their roles and responsibilities and the required access to clinical and/or business information. All staff are provided appropriate training in the relevant computer software and the potential risks before access and passwords are provided.

It is the responsibility of the the Computer Security Coordinator to create users as well as the removal of access rights of any member of the team who leaves the practice. E.g. by the decommissioning of passwords, remote access logins, and the return of computer equipment, backups and entry devices (keys) to the practice. The Computer and Security Coordinator also to manages guest or remote access rights. Access rights and reviews for completeness and accuracy of user information is done 6 monthly.

Password Management

- Practice team members have individual passwords (not generic), which are kept secret and secure. 'Strong' passwords are used and the practice team are trained in the importance of this.
- Individual practice team members are assigned an appropriate access level specific to their role.
- Default user accounts removed except for system administrator
- Access rejected after three invalid attempts and rest required by system administrator.
- Passwords are changed every three months.
- A minimum length is set (i.e. number of characters).
- A mixture of alphabetic and numeric characters and lower and upper case is used.
- Passwords do not use familiar and family names or words that can be found in a dictionary.
- Dates of birth are not used.
- Passwords are not reused.
- Passwords are not disclosed to anyone and others are not allowed to use your login.
- Passwords are not written down and attached to screens.
- Logins are not shared (i.e. people in the same role do not use the same username and password).

Auditing of access information is enabled and actions performed are identifiable by individual user. The audit logs are reviewed periodically.

The website content is accessed and managed by Laura Fitzgerald (Receptionist)

Helpful Resources:

Australian Privacy Principles

Business Continuity and Information Recovery

Policy

Our practice has a business continuity plan in place in the event of an emergency such as power failure to ensure the information on the computers is saved and protected.

Our practice uses the business continuity plan attached.

Some of the functions which need to continue when a computer 'disaster' occurs are:

- Making appointments for patients
- Giving patients invoices and receipts
- Allowing Practitioners to provide adequate clinical care while not having access to electronic health records
- Knowing who to contact for technical advice on getting the system operational again

- Knowing how to restore data using the backup medium, and, together with technical support, ensuring that computer hardware and software are restored to normal working conditions
- Outlining any of the additional roles that staff might need to undertake during the disaster.

Procedure

Our business continuity plan is stored in the Practice Manager's office, offsite and on PracticeHub.

To ensure that quality consultations continue in the event of computer failure, our practice prints templates from the clinical software program and stores in a central location. These can then be used as part of the consultation with hand written notes scanned or entered into the clinical software when the computers come online.

The plan was last updated 2017 and discussed at regular practice meetings.

The Computer Security Coordinator is responsible for testing and updating the disaster recovery plan on a six-monthly basis.

Useful Link:

Australian Privacy Principles - https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

Information Backup

Policy

To avoid loss of data, the data held on our practice's computer system is automatically backed up regularly with the backups periodically tested to verify that the data can be restored if necessary.

All backup media is stored securely when in use and destroyed when no longer used.

Backup media

Data files are the files that have been created by our practice, as opposed to system files, which are the software programs. Programs can be restored from the original disks, but data files cannot be restored unless there is a restorable backup copy.

Our practice backups all data files (including clinical, financial and administrative data) and system data on to removable media. Our practice uses a system of daily, weekly, monthly and annual backup.

Procedure

Our practice uses tape media and mirrored drives to perform computer system backups. It is the responsibility of the Practice Manager and the IT service provider for backing-up data on a daily basis and that data is transferred from old backup technology to current technology where necessary.

A full backup of the system in addition to the daily backup is performed on a weekly, monthly and annual basis.

All backups and archived data are encrypted and password protected.

Backup media is securely stored *onsite* on mirrored hard drives, on tape and on workstations and is protected from theft, water and fire damage. Backup media is securely stored *offsite* every with the Practice Manager and is protected from theft, water and fire damage. It is the responsibility of the Practice Manager for storing backups securely offsite away from heat and magnetic fields.

To ensure that data backup is working, our practice performs a 'trial restore' on a monthly basis.

Restoring procedure in the event of a server failure

- Locate backup media for the previous day
- Insert backup media in the server
- Ensure that all other computers have logged out of the server
- Perform restore for particular system/files
- Check that the system/files restored look correct (name, size and date)
- Check that the system functions correctly Remove backup media and store in secure location

Malware, Viruses and Email Threats

Policy

Our practice has reliable protection against computer malware and viruses.

Procedure

Our practice uses *anti virus and anti-malware software* on all computers and mobile devices that connect to the practice system and ensures the following:

- all computers attached to the practice network have installed and fully enabled virus and malware checking software
- that malware protection software is not disabled or bypassed, nor the settings adjusted to reduce their effectiveness. This means that general users of the system are not authorised to alter these settings
- automatic updating of malware protection software and its data files are enabled for daily updating.
- automatic scanning of all email attachments
- automatic scanning of all documents imported into the computer system

- nightly scanning of all computers
- practice team members are trained in malware prevention procedures
- practice team members are trained in malware detection and to report all incidents
- the cookies feature in web browsers are turned off

Approval is sought from the Practice Manager/Computer Security Coordinator before any removable media is inserted into the practice computers.

Useful Resources:

Australian Privacy Principles

Computer Network Perimeter Controls

Policy

Our practice has network perimeter controls to protect the practice system by analysing data entering and leaving our network. Our practice uses multiple protection mechanisms, such as firewalls, intrusion detection systems, virtual private networks (VPNs), content filtering and antivirus protection.

Procedure

In our practice, the type of firewall we have is recommended by our IT solutions provider and upgraded as necessary.

The firewall is tested on a monthly basis and all long files are routinely examined. The person responsible for testing the firewall is the Computer Security Coordinator and the IT solutions provider.

All software and hardware used to protect the system is noted in our equipment register.

Useful Resources:

Australian Privacy Principles

Mobile Electronic Devices

Policy

Our practice has processes in place to ensure the safe and proper use of mobile electronic devices including portable devices such as USBs, removable hard drives and portable electronic clinical equipment.

Procedure

All portable devices are to be password protected, encrypted and stored securely where possible.

List of Mobile Devices	Mechanism for securing its data
Toshiba Laptop	Password protected, anti-viral software, firewall software, etc.
Samsung Tablet	Password protected
Samsung Android Phone	Password protected

Useful Resources:

Australian Privacy Principles - https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

Practice Facilities and Computer Hardware, Software and Operating System

Policy

In our practice, the staff member responsible for computer system maintenance is the Practice Manager.

In our practice, computer system maintenance is conducted on a monthly basis.

Our practice upholds a clean desk and clear screen policy.

Procedure

To protect against data corruption, our practice has an uninterruptible power supply (UPS) on the server PC to prevent unexpected shutdowns in the event of a mains power failure. The batteries in the UPS are checked regularly.

Electrical surge protection filters are used to protect our practice's PCs and other hardware from power fluctuations and failures.

Disks and computer equipment is positioned away from environmental hazards such as extreme heat or cold, direct sunlight, high or low humidity and magnetic fields.

GPs and staff members exercise care to safeguard electronic equipment and data assigned to them. If reasonable care is not taken, they may be accountable for any loss or damage that occurs.

Computer equipment is maintained on a [monthly] basis including:

- checking remaining hard disk drive capacity
- checking logs for errors
- checking for the installation of unauthorised programs
- reviewing anti-virus scanning software to ensure it is working effectively and to make sure that the latest update is installed on all machines
- defragmenting the hard drive
- deleting temporary files
- cleaning around the fans of the computers so that dust does not accumulate (refer to the manufacturer's instructions).
- securing all equipment from theft
- ensuring the secure disposal of hardware, in particular where it may contain clinical and/or business information. This includes securely deleting all data from the device.

Physical access to the server is restricted and is locked in a safe place. Password access to the server is also limited to key members of the practice team as determined by the Practice Manager.

Software maintenance is completed on a regular basis including:

- Patching to keep software up to date
- Reviewing user access
- Checking for installation of unauthorised programs
- Software configuration: installing and maintaining software in accordance with the vendor’s guidelines to ensure security is maintained. Including ensuring that auditing is turned on to log operating system and application activity
- Running file integrity software
- Keeping a software maintenance log.

Clear Screen

Some healthcare professionals like their computer screens to be clearly visible to their patients during consultations. It is important to be vigilant about inappropriately exposing information to a third party, for example it might not be acceptable for a parent to see the past history of their adolescent child. More importantly, patients must not be able to view the clinical record of another person (e.g. the patient previously consulted). Similarly, receptionists need to be careful that patients do not have inappropriate visual access to any information on computer screens at the front desk.

To protect confidentiality, staff are to:

- use ‘clear screen’ function keys, which instantly close down an open file or switch off the monitor
- use password protected screensavers (suggested default of 15 minutes)
- log off when leaving workstations
- exit the previous patient’s electronic file before the next patient enters the consulting room
- remove documents from printers and faxes immediately

Clear Desk

At the end of each day each practice team member is to clear their desks of all documents, notes and media.

Privacy Audit

Privacy audit is to be conducted weekly, ensuring continuity to privacy and confidentiality is maintained

Useful Resources:

Australian Privacy Principle 11: Security of personal information

Security for Information Sharing

Policy

In our practice, all patient-related information sent electronically between healthcare providers is sent by secure message delivery. Confidential data is not to be sent via email or the internet.

Procedure

Our practice uses Best Practice secure messaging system.

Healthcare Identifiers
All staff are trained and regularly updated on the use of healthcare identifiers. The *Healthcare Identifiers Act 2010* stipulates that reasonable steps must be taken to protect the identifiers from misuse, loss and unauthorised access, modification or disclosure. The healthcare identifier for an individual is taken to be personal information and therefore is also subject to the *Australian Privacy Act 1988.*

Digital certificates
Our practice has two PKI certificates: a Medicare claims and payments certificate for HI Service access and a National Authentications Services for Health (NASH) PKI certificate to access the national *My Health Records* system and for secure message delivery. These certificates authenticate, encrypt and seal the message and can also be used to connect to national repositories. All certificates are stored securely and the expiry of each recorded and a record is kept of which certificate is installed on which computer and device.

Practice website safety and security
Information on our practice website is up to date and does not invite unsafe practices. Our website is hosted separately from practice data.
The practice must abide by the Guidelines for Advertising of Regulated Health Services set by the Medical Board of Australia.

Helpful Resources:
Australian Privacy Principle 9: Adoption, use and disclosure of government related identifiers.

Data Security

Policy

Data security in the consulting room is more about GP activities than technical matters. For example, some GPs like their computer screens to be clearly visible to their patients during consultations.

GPs need to consider if there might be sensitive information on the screen which must not be seen. Examples include parents seeing a sensitive past history of their teenage child such as a sexually transmitted disease, or patients viewing the clinical record of the person previously consulted.

Similarly, receptionists need to be careful that patients do not have visual access to confidential information on computer screens at the 'front desk'.

There are various methods by which the information can be kept confidential. Some have to do with screen positioning, but screensavers and the use of a function key which instantly closes down an open file, are useful technical options.

For ensuring backups are stored securely, refer to **Backup and restore**.

Helpful Resources: eHealth

Procedure

In our practice, we keep personal health information secure by use of screensavers, anti-viral software, passwords, firewall, data backups and regular maintenance.

Secure Messaging

Policy

The purpose of this policy is to give guidance on the use of secure messaging by all staff working in the practice.

The specific aims of this policy are to outline:

- How, when and by whom secure messaging is used
- To whom secure messaging communicates with
- Maintenance of the secure messaging software
- How the use of secure messaging is promoted

Procedure

Roles and Responsibilities

The **practice principal** has the responsibility of making final decisions regarding secure messaging products and usage. It is also their responsibility to encourage and support the use of secure messaging within their organisation. The practice principal is also the Responsible Officer (RO) in matters relating to the Healthcare Identifiers (HI) Service.

It is the responsibility of the **practice manager** to maintain the day-to-day running of secure messaging software, and troubleshoot or report any problems that may arise to the appropriate secure messaging software vendors. In conjunction with the practice principal, it is also the responsibility of the practice manager to promote the use of secure messaging by maintaining eHealth contact information with external organisations/professionals. The practice manager is typically the Organisational Maintenance Officer (OMO) in matters relating to the HI Service. The practice manager is responsible for reviewing this policy, ensuring that it is up to date and distributing it to all relevant staff members.

It is the responsibility of the **healthcare professionals** to send health information using secure messaging in a way that is out outlined in this policy.

Administration staff have the responsibility of supporting the use of secure messaging by undertaking any administration tasks involved in the maintenance or use of secure messaging by other staff members.

Principles

Using secure messaging

Messages sent from this practice to external healthcare professionals and organisations will be sent using secure messaging in preference to using fax, letters etc. where possible.

Training and education

Training on the procedures involved with electronic secure messaging and how to use secure messaging software will be provided to all existing staff and all new staff at the practice. If there are significant updates and changes to electronic secure messaging and its software, all staff will be informed and re-trained where necessary.

Promoting the use of secure messaging

The Practice will advise external healthcare professionals/organisations that the practice's preferred method of communication is via standards-compliant secure messaging. For example the practice will make available our secure messaging contact details, which will allow others to be aware of how to communicate with our practice via secure messaging.

Our practice will ensure that all secure messaging contact details on the Healthcare Provider Directory and Endpoint Location Service are accurate and up to date.

Secure messaging maintenance

The practice will choose, install, configure and use secure messaging software that is compliant with NEHTA standards.

The practice will diligently ensure that secure messaging software is up to date and operating at the most current version, allowing us to send or receive all new types of messages specified by NEHTA.

When any problems arise with the secure messaging software within our practice, the appropriate secure messaging software vendor will be contacted to try and resolve the problem in a timely fashion.

Online Security and Technology

Policy

Medicare Australia has developed a security system for health care electronic transactions using Public Key Infrastructure (PKI) technology. Using digital certificates, transactions can be digitally signed and encrypted and sent to Medicare Australia and other health professionals and locations that also have PKI. This technology is intended for use across the entire Australian health sector.

There are two types of digital certificate used in Medicare Australia's PKI:

- Location certificates which relate to a building, location or the practice
- Individual certificates for persons who will be corresponding electronically with Medicare Australia and other health care professionals and locations.

For most practice situations, a Location certificate for the practice and Individual certificates for GPs and some key staff members is required. If Individual certificates are used, a Location certificate is also required. Both Location certificates and Individual certificates need to be associated with a valid unique email address. Certificate details are stored on a token (a Smart Card or Key Ring).

Firewalls

A firewall is an electronic mechanism that blocks unauthorised access into a computer system. These can be in the form of software or hardware. Various programs, some of which are freely available on the internet, can be installed to protect the computer network from 'hackers'.

Similarly, hardware can be added to the computer system so that it acts as a protective device between the computer and the internet. It stops the inbound (and sometimes the outbound) passage of certain packets of data and can prevent unauthorised access from specific sites.

Procedure

In our practice, the type of firewall we have is recommended by our IT solutions provider and upgraded and as necessary.

Our IT solutions provider will test the firewall on a monthly basis.

Helpful Resources:

RACGP Computer Security Guidelines

eHealth

Office of the Australian Information Commissioner

Medicare Australia

Secure Communications

Procedure

Internet and email users are responsible for ensuring that the provided facilities are used in an effective, ethical and lawful manner. Internet and email users do not use the internet and email for purposes that are illegal, unethical, harmful to our practice or the medical profession or non-productive. Acceptable use includes obtaining information from medical and business websites, using email for practice business, and accessing online databases.

Unacceptable use includes forwarding chain emails and viruses, transmitting copyrighted materials without permission, visiting websites with obscene or objectionable content; transmitting any offensive, harassing or fraudulent messages or conducting personal business.

Any executable files downloaded from the internet or by email (e.g. software patches or any files with an .exe, .bat or .com extension) are scanned for viruses following download.

As information from the internet can be outdated, incorrect or misleading, any information obtained from the internet is verified for accuracy with other information sources before being used.

Confidential information is not sent over the internet unless encrypted.

All practice staff, medical practitioners and allied health professionals working within the practice and using the practice's technology resources are required to sign an Internet and Email Usage Policy as part of their Contract of Employment

Scanning Documents and Digital Media

Policy

The current legal position is that the original document is the best evidence. In the absence of an original document, the court has to be convinced that a copy is a true copy of the original and the person responsible for computerised records may be required to give details on what happened to the original document. In the case of images created using a digital camera, these images are the original document.

To be able to dispose of original documents once scanned and present an electronic document or digital image as evidence, it is necessary to prove:

- Scanning and/or recording digital images are a normal procedure for storing patient information for our practice
- When the document or image was created, e.g. document or image is time and date stamped
- Who created the document or image and that this person was capable and responsible
- There is a defined procedure for creating and checking electronic documents
- The system that created the document or image was not susceptible to tampering or hacking (i.e. the document could not be edited)
- Audit logs are available to track access.

As a result, it is strongly recommended that the GP or practice contact their medical defence organisation for their advice.

Procedure

In our practice, we scan patient correspondence received into the patient's electronic record.

Our scanning processes consist of the following steps:

1. Use the front scanner for faxing/scanning
2. Stamp paperwork (e.g., Script, referrals, correspondence) with “Scanned” Stamp, date & initial (before scanning)
3. Stamp with the “Received” and “Scanned” stamp if it is **mail**, date & initial (before scanning)
4. Put the paperwork into the copier, face up, top of paperwork in first
5. To scan paperwork into computer

Scanning Procedure (once in computer)

1. Click on file icon on the bottom of the screen
2. Open Shared Data (S:)
3. Open Scan folder
4. Rename file that was scanned in
5. Send via fax or email
6. Do NOT delete file before checking to see if scanned into patient’s file
7. Click on the disc symbol at the bottom of the screen
8. Click on the import document button at the top left-hand corner of the screen
9. Select the document from the Scan folder you wish to upload
10. If wanting to send to doctor’s inbox, ensure it is clicked on “inbox” otherwise if paperwork is to be placed into patients file click on “patients file”
11. Click search, select patient you wish to import document into
12. In the subject field, type in what the paperwork is (E.g., Medical records, referral, script).
13. Ensure “store in” is selected on correspondence in
14. Click on the user field – this is the doctors inbox you are wanting to import paperwork into
15. Click on the category and choose the description of the paperwork (E.g., Referral would go under referral letter)
16. Tick “delete file after importing
17. Click “ok”
18. If multiple pages have been uploaded, click next and repeat steps 10 - 17.