Information Technology (IT), PCEHR, Privacy, Email, Social Media and Data Breach

Family Doctor Service (FDS) Information Security (IT) Policy

Introduction

WHO IT APPLIES TO: All workers.

CONSEQUENCES OF BREACH:
Breach of this policy will be dealt with in accordance with the relevant FDS employment agreement and may lead to disciplinary action including possible termination of employment.

For contractors who are found to have breached this policy, there may be consequences including termination of contract. Where inappropriate use under this policy constitutes a breach of any law, action may also be taken in accordance with that law by the FDS or concerned third parties.

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

Goran Mujkic has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

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

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

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

- We have a business continuity plan that has been developed, tested, and documented.
- Electronic data transmission of patient health information from our practice is in a secure format.
- Our practice has the following information to support the computer security policy:
- Current asset register documenting hardware and software including software licence keys.
- Logbooks/printouts of maintenance, backup including test restoration, faults, virus scans.
- Folder with warranties, invoices/receipts, maintenance agreements

This Practice reserves the right to check individual's Computer System history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the Practices Computer Systems or breaches of Practice Computer Security will be fully investigated and may be grounds for dismissal.

This practice has a sound backup system and a contingency plan to protect practice information in the event of an adverse incident, such as a system crash or power failure. This plan encompasses all critical areas of the practice's operations such as making appointments, billing patients, and collecting patient health information. This plan is tested on a regular basis to ensure backup protocols work properly and that the practice can continue to operate in the event of a computer failure or power outage.

This policy and supporting policies provide staff with instructions and guidance concerning Information Security allowing a consistent and appropriate approach to protecting the information assets of the organisation.

Scope

This policy applies to the Records managed network and/or owned network components. This includes, but is not limited to:

- The Primary Firewall
- All servers
- All FDS equipment (laptops, workstations, etc.)
- Routers connecting networks.
- Remote sites workers
- Devices connecting to FDS owned equipment.

Definitions

Information Technology (IT) and IT Security use specific terms that may not be known to all. The concepts are described here.

Information Security

Information Security is the term used to describe the "the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use".

The goals of information security are to provide Confidentiality, Integrity and Availability (CIA). These three concepts are central to information security and must be always kept in mind when implementing technology.

- **Confidentiality –** the assurance that only authorised users have access and can manipulate the information.
- **Integrity –** the information provided is accurate and has not been tampered with
- **Availability –** The required systems and the information, is available to those that require access when needed.

Policy, Standards, Guidelines & Procedures

There is often some confusion as to what the exact purpose of a specific type of document is.

Within State Records, the following definitions will be used:

- **Policy -** An Information Security policy is a management instruction that outlines the role of Information Security within FDS, what the roles, and responsibilities of staff is, and provides guidance on security issues. The policy contains high level statements that are mandatory. The Information security policy consists of this document and supporting issue specific documents.

- **Standards -** Standards contain the specific requirements that must be met. They provide information on how the organisation should implement/perform certain functions. Internal to the organisation there may be additional standards that should be followed.

- **Guidelines -** Unlike policies, guidelines are optional. They are highly recommended and should be followed. For example, the Password selection guidelines while not mandatory, are highly recommended to be used to select a strong password.

- **Procedures -** Procedures state how the standards, guidelines and policies are to be implemented. They are often detailed instructions on how to perform a certain task. Policies are high level documents outlining what must be done, standards provide information on how the policy can be met, and guidelines support the standards and policies. Finally, procedures state how they can be implemented and provide detailed instructions.

Compliance with policy

Compliance

This information security policy applies to:

- All computer systems owned and/or managed by FDS, regardless of their location.
- All platforms (operating systems) deployed within the organisation.
- All computer sizes, ranging from Personal Digital Devices (PDA) through to corporate servers.
- All information handled by FDS systems.
- All applications and systems whether developed by FDS or purchased.
- All FDS staff that use FDS computing facilities, this includes but is not limited to full time employees, part-time or casual employees, contractors, subcontractors, consultants, etc.

All staff members are expected to be familiar with and comply with this policy. Violations of this policy can lead to revocation of system privileges and/or disciplinary action up to and including dismissal. Unlawful activities may be referred to the appropriate authorities for criminal/civil action.

Compliance Audits /Review and evaluation

For the Information Security Policy to remain effective, it must be reviewed regularly, updated when changes are made and compliance with the policy evaluated on a regular basis.

Compliance with this policy must be evaluated at least once every twelve (12) months. This review must keep in mind:

- Changes in technology
- Effectiveness of current policy and controls (this can be determined by the number and Nature of any security incidents recorded)
- Cost and impact of controls on the business

Responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined. See Template 2.1.

All staff within the organisation have some responsibilities concerning Information Security. Additional details regarding roles and responsibilities are provided in Template 2.1.

Information security is not only a technological issue, but also a human issue. The human Resources (HR) department plays an essential role in managing security. HR has the responsibility to:

- Verify information on applications, e.g. Reference check
- Ensure that all staff have signed a confidentiality agreement before commencing work.
- Notify CIC of new employees and terminations.
- Ensure documentation such as the confidentiality agreement and terms and conditions are understood and have been signed by staff.

Third Party Access

There will be occasions when third parties require access to FDS resources to conduct business, perform maintenance tasks, or to deliver services. To protect the environment all third-party access must:

- Be authorised by the appropriate system owner.
- In the case of new connections, have risks evaluated before connecting.
- Connect in accordance with the access control policy.
- Be made aware of their responsibilities regarding security.
- Be covered by a formal agreement which includes security requirements.
- Be covered by a confidentiality or non-disclosure agreement.

Asset Inventory/business continuity

To protect assets, they must first be identified and valued. An inventory of important assets must be created and maintained. Owners must be clearly identified.
The assets to be documented should be:

- All information assets: databases and data files, system documentation, user manuals, Training material, operational or support procedures, continuity plans, fallback Arrangements, archived information
- All software assets: application software, system software, development tools and Utilities
- All physical assets: computer equipment (processors, monitors, laptops, modems) Communications equipment (routers, pabxs, fax machines, answering machines)
- All personal assets: information on the skill required to maintain and manage the Systems in use within the organisation.
- A business continuity and disaster recovery plan must be documented in case of server Crash or disaster happening.

Responding to security incidents and malfunctions

Security incidents, weaknesses and software malfunctions must be reported to computer security coordinator and recorded in the system as soon as possible after the incident is discovered. By recording these incidents management can be provided with accurate security and fault details. This allows FDS to correct the issue and minimise the impact the incident or malfunction may have on the organisation.

Physical and environmental security

- To protect computing resources from accidental or deliberate damage physical access to those machines will be restricted to those that require access.
- You may not divulge, copy, release, sell, loan alter or destroy any information unless authorised by the principal.
- You must safeguard any physical key, ID Cards computer network account that allows you access to FDS information. This includes creating difficult to guess passwords.
- Information must be erased from equipment prior to disposal or re-use.
- You must also destroy or render unavailable any confidential information contained in any physical document (e.g memo, report or any electronic, magnetic, or optical storage medium before it is discarded).

Security of equipment off-premises

Equipment may be taken off site for several reasons. A laptop assigned to a staff member, equipment sent for repair to a vendor, etc. Equipment to be taken off-site, i.e. removed from FDS controlled premises, must only be taken when authorised to do so. Before removing equipment off premises, a log entry must be made to record removal of the item. Reasonable steps must be taken to ensure the safety and security of the equipment and the data contained on it whilst it is off premises.

Communications and operations management

To ensure the correct and secure operation of information processing facilities:

- Controls will be in place to protect the network from unauthorised access.
- Changes to processing facilities must be controlled and implemented according to the change management procedures.
- Procedures identified in this policy and supporting policy must be documented and maintained, including incident management procedures.
- Development and production environments must be separate.
- Duties, where required and feasible should be segregated.
- External facilities must be used with care and only after the risks have been identified and
- Appropriate controls agreed; capacity on critical systems must be monitored.
- All data and systems on production servers must be backed up regularly and off-premises.
- Copies kept.
- Operational staff must maintain a log of their activities.
- Faults shall be reported, and corrective action taken.

Malicious Software

Malicious code or software such as viruses, Trojans, logic bombs, and blended threats can cause a lot of damage, both in lost time as well as through destruction of important information. To prevent this FDS has anti-virus products to scan and clean all transmissions into and out of the organisation. Staff must take care when accessing the Internet and using floppy disks or other removable media to transfer information to FDS's workstations.

It is the policy of FDS to implement controls on hardware used to fulfil the needs and conduct FDS business, to prevent Malicious Software from disrupting the medical center operations.

The controls are as follows:

- Anti-virus and anti-spyware/anti adware software must be installed, active and maintained with up-to-date definitions on all workstations, laptops, and servers.
- All files should be scanned n real time each time they are accessed including those located on removable storage devices, floppies, CD's, and network stores.
- When malicious software or threat is found, the suspected files must be automatically removed from the system.
- All e-mail messages and attachments should be scanned for malicious software.
- Files downloaded from the Internet via the firewall should be scanned for malicious software.
- Server malicious software log files must be generated and maintained for a period of 1 Year with 3 months of data online.
- If any users suspect that any malicious software is present on their workstation laptop or a server, they should contact their computer security coordinator immediately.
- User must report any other suspicious activity to their computer security coordinator (e.g. Erratic mouse movements, browser windows opening unexpectedly, etc).

Exchanges of information and software

Sensitive information is exchange with third parties and must be protected by agreements.

- **Post -** must be addressed private and confidential to person concerned. If patient records are being sent must be sent by registered mail only after signed permission received.
- **Fax -** must use a cover sheet with disclaimer and addressed private and confidential. If any information is highly confidential phone first to the person concerned so that they can take the fax straight off the machine.
- **Email -** no sensitive information is to be sent by email as it is not encrypted. If a patient requests information by email advise that it is not secure.
- **SMS -** no sensitive information to be sent via SMS excepting recall and reminder unless patient does not consent.
- **Twitter, or similar -** not to be used.
- **Video, or similar -** only used for Telehealth, and have a dedicated private room for consultation.
- **Phone -** face to face and phone consultations can be easily overheard, so confidential information should never be discussed unless in a private area. Messages left on answer machines, only state please call ..... on the phone number.

Access control

1. **User authentication and passwords.**
   a) All FDS information systems providing services to staff, doctors, or external parties, may only be accessed by authorised information users.
   b) The respective information owner will govern the access rights of users for each system.
   c) All users, utilities and applications must go through a user authentication process before being given access to any system.
   d) Access shall be restricted to those capabilities and information that are appropriate to each user's role within FDS's business environment. See template 4.1.
   e) As a minimum, access to each information system, shall be controlled by a log on identification (LogonID) and password-based security system.
   f) Each user must be able to be uniquely identified by the LogonID.
   g) Passwords should be changed on a regular basis and not be obvious (easy to guess).
   h) A single sign on system, providing access to multiple information systems, via one LogonID, shall be made available to certain groups of users, where it does not pose a security risk to FDS, and it is feasible to do so. This is for windows log on.

2. **Network access control and firewalls.**
   a) Access to all FDS's systems shall be automatically monitored and controlled via an intrusion detection system, for unauthorised intrusion and to ensure all users are only accessing information systems they are authorised to do so.
   b) Access to all information systems running on FDS's networks must be through a firewall facility. A restrictive policy for firewall parameters shall be adopted, so that all services are denied unless specifically permitted.
   c) Access to FDS's network components will be segmented and segregated according to the nature of users accessing systems on that segment.

3. **Operating system access control.**
   a) The security features at the operating system level shall be used to restrict access to computer resources to only those users or applications authorised to do so by the information custodian.
   b) Access to any operating system files and utilities must be in accordance with the user authentication requirements of this policy (7a above).

4. **Application access control.**
   a) Access to application system files, systems utilities and databases shall be in accordance with the authentication policy outlined above.

Internet, social media, and email

The FDS recognises the usefulness of the internet, email, mobile devices and computer equipment as research, communication, and work tools. This policy sets out the appropriate standards of behavior for users of the FDS's information technology resources.

At all times when accessing or using the FDS's information technology resources, users must ensure that they comply with this policy. It is the user's responsibility to ensure that they use the FDS's information technology resources in a lawful and professional manner.

This policy outlines the expectations in the use of the FDS's:

- Information technology resources.
- Internet.
- Social media.
- Email facilities.
- Mobile phones and mobile devices.

If a user is unsure about any matter covered by this policy, they should seek the assistance of their manager.

This policy applies to all staff members of FDS, and contractors (including sub-contractors and temporary contractors) referred to as users. This policy applies to the use of all internets, social media, email, and computer facilities, both during and outside of business working hours.

This policy applies to the use of internet, social media, email, and computer facilities inside the workplace, as well as use from remote locations and after hours use of personal computers. Use of computer facilities includes use of laptops, mobile phones and similar products, and any other equipment that provides a means of accessing the FDS's email and internet facilities.

For example, this policy extends to the use of a personal computer which has access to the FDS's IT systems.

The FDS's information technology resources ("IT resources") are provided to support the Business and administrative activities of the FDS.

These resources include:

- The FDS's network.
- Computer systems and software including personal computers, notebooks, and servers.
- Mobile phones, smart phones, and wireless data cards.
- Access to the internet.
- Email, telephones, and related services.

If users produce, collect and/or process FDS related information in the course of their work, that information remains the property of the FDS. This includes information stored on third party websites.

Extent of personal use

Users are permitted to use the FDS's IT resources for limited, incidental personal purposes, provided that such use does not:

- Interfere with the efficient business operations of the FDS.
- Violate this policy or any other policy of the FDS.
- Negatively impact upon the user's work performance.
- Hinder the work of other users.
- Damage the reputation, image, or operations of the FDS.
- Such use must not cause noticeable additional cost to the FDS.
- The FDS accepts no responsibility for:
    - Loss, damage or consequential loss or damage, arising from personal use of its IT resources.
    - Loss of, or interference with personal files arising from efforts to maintain the IT resources.

Guidelines for use of IT resources

Users must comply with the following guidelines when using the FDS's IT resources:

- Users must use their own username/login code and/or password when accessing the FDS's computer systems.
- Users should protect their username, login code and password information always and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.
- Username/login codes and passwords are not to be recorded on or near computer equipment/mobile devices.
- Users should ensure that they log off from their account and lock their computer/mobile device or shut down their computer/mobile device when leaving such equipment unattended to ensure that others do not have access to the FDS's computer systems.
- Users in possession of the FDS's computer equipment or mobile devices (including laptops, mobile phones, pagers, personal data assistants, wireless data cards, etc) must always ensure that such equipment is stored or placed in areas with a minimal possibility of theft or damage.
- IT resources must not be used for private commercial purposes except where the paid work is conducted in accordance with the FDS's practice, or the work is for the benefit of an entity in which the FDS holds an interest.

- Use of proprietary software is subject to terms of license agreements between the FDS and the software owner or licensor and may be restricted in its use.
- The FDS name or logo may only be used with prior approval from the Principal.

All use must be in accordance with the prior approval of the Principal.

Prohibited conduct

Certain behavior is inappropriate use of the FDS's IT resources and is strictly prohibited.

Examples of such prohibited conduct are, but are not limited to:

1. Users must not send (or cause to be sent), upload, download, use, retrieve, or access any file, email, or internet material that:
    a) Is obscene, offensive, or inappropriate. This includes text, images, sound, or any other material, sent either in an email or in an attachment to an email, or through a link to an internet site (URL). For example, material of a sexual nature, hateful, indecent, or pornographic material.
    b) Causes insult, offence, intimidation, or humiliation by reason of unlawful harassment or discrimination.
    c) Is defamatory or incurs liability or adversely impacts on the image of the FDS. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people.
    d) Is otherwise illegal, unlawful, or inappropriate.
    e) Affects or may affect the performance of, or cause damage to or overload the FDS's computer systems or internal or external communications in any way.
    f) Gives the impression of or is representing, giving opinions, or making statements of on behalf of the FDS without the express authority of the FDS.
    g) They do not solicit socially harmful activities including arms, carbon pollution, gambling, tobacco, pornography, low-cost labor/ slave labor, human rights violations and animal cruelty.

2. Users must not use IT resources to:
    a) Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using the FDS's computing facilities, except as permitted by law or by contract with the owner of the copyright. Similarly, users should not copy, or access copyright protected music or videos on the FDS's IT resources.
    b) Breach an individual's privacy, including patients under the care of a Fellow or trainee.
    c) Create any legal or contractual obligations on behalf of the FDS unless expressly authorised by the Principal.
    d) Disclose any confidential information of the FDS or any employee, Fellow, trainee, client, or supplier of the FDS unless expressly authorised by the FDS.
    e) Install software or run unknown or unapproved programs on the FDS's computers. Under no circumstances should users modify the software or hardware environments on the FDS's computer systems (this includes installing software purchased by users for personal private use) without prior approval from the general manager, IT.

f) Gain unauthorised access (hacking) into any other computer within the FDS or outside the FDS or attempt to deprive other users of access to or use of any FDS computing system.
g) Plagiarise another person's work.
h) Deliberately send or cause to be sent chain or spam emails in any format.
i) Obtain personal gain. For example, running a personal business using the FDS's computers.
j) Gamble.
k) Stream content for personal use.
l) Use peer to peer file sharing software such as VUZE, BitTorrent, etc.
m) Download, install or use instant messaging software.
n) Perpetrate any form of fraud or software, film, or music piracy.

Users must not use another user's computer or internet access or email facilities (including passwords and usernames/login codes) for any reason without the express permission of the user.

Internet

The FDS's IT resources should only be connected to the internet using means authorised by the Principal, IT.

Users are not permitted to publish personal web pages on computers connected to the FDS network.

Using social media in our practice Policy

'Social media' is defined as online social networks used to disseminate information through online interaction.

Regardless of whether social media is used for business related activity or for personal reasons, the following standards apply to members of our practice team, including general practitioners.

Practitioners and team members are legally responsible for their postings online. Practitioners and team members may be subject to liability and disciplinary action including termination of employment or contract if their posts are found to be in breach of this policy.

Personal and professional use of social media by FDS staff and contractors must not bring the FDS into disrepute, compromise effectiveness at work, imply FDS endorsement of personal views or disclose, without authorisation, confidential information.

Workers are responsible for the content they post on their personal social media accounts. Where a Worker's personal use of social media contravenes our policy, then it may be appropriate for the FDS to respond, either in work time or after hours.

Think about consequences, please remember: Using your public voice to trash or embarrass your employer, your patients, your co-workers or even you are not okay - and not very smart.

For the sake of clarity, social media includes, but is not limited to:

- Social networks (such as Facebook and MySpace).
- Blogs.
- Wikis (such as Wikipedia).
- Podcasts.
- Forums.
- Content communities (such as YouTube and Flickr).
- Microblogs (such as Twitter).

Procedure

Our practice has appointed Practice Manager Goran Mujkic as our social media officer with designated responsibility to manage and monitor the practice's social media accounts. All posts on the practice's social media websites must be approved by this person.

When using the practice's social media, all members of our practice team will not:

1. Post any material that:
   a) Is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, or offensive.
   b) Infringes or breaches another person's rights (including intellectual property rights) or privacy, or
   c) misuses the practices or another person's confidential information (e.g. do not submit confidential information relating to our patients, personal information of staff, or information concerning the practice's business operations that have not been made public)
   d) Is materially damaging or could be materially damaging to the practice's reputation or image, or
   e) another individual
   f) Is in breach of any of the practice's policies or procedures.

2. Use social media to send unsolicited commercial electronic messages or solicit other users to buy or sell products or services or donate money.

3. Impersonate another person or entity (for example, by pretending to be someone else or another

4. practice employee or other participant when you submit a contribution to social media) or by using another's registration identifier without permission.

5. Tamper with, hinder the operation of, or make unauthorised changes to the social media sites.

6. Knowingly transmit any virus or other disabling feature to or via the practice's social media account, or use in any email to a third party, or the social media site.

7. Attempt to do or permit another person to do any of these things:
   a) Claim or imply that you are speaking on the practice's behalf unless you are authorised to do so.

b) Disclose any information that is confidential or proprietary to the practice, or to any third party that has disclosed information to the practice.
c) Be defamatory, harassing, or in violation of any other applicable law.
d) Include confidential or copyrighted information (e.g. music, videos, text belonging to third parties), and
e) Violate any other applicable policy of the practice.

All members of our practice team must obtain the relevant approval from our social media officer prior to posting any public representation of the practice on social media websites. The practice reserves the right to remove any content at its own discretion.

Any social media must be monitored in accordance with the practice's current polices on the use of internet, email, and computers. Our practice complies with the Australian Health Practitioner Regulation Agency (AHPRA) national law and takes reasonable steps to remove testimonials that advertise our services (which may include comments about the practitioners themselves).

Our practice is not responsible for removing (or trying to have removed) unsolicited testimonials published on a website or in social media over which we do not have control.

Any social media posts by members of our practice team on their personal social media platforms should:

- Users must take a commonsense approach to the content that they publish online. Because of the public nature of the internet and social media, this commonsense approach also applies to use of social networking sites outside of business hours or on equipment other than FDS equipment.

- If a user is holding themselves out as a representative of the FDS, any material published online must:
  - Be relevant to the user's area of expertise.
  - Not be anonymous.
  - Maintain professionalism, honesty, and respect. Statements of fact about the FDS and its products and services, publicly available information and information already published on the FDS's website (when available) are all examples of appropriate online content.

- Users must not publish any material online that contains the FDS's confidential information (including financial information and information about organizational matters), the personal information of another (without that individual's consent), information about the FDS's customers or clients, or content that may offend, intimidate, defame, or humiliate a Fellow, trainee, staff member, volunteer, or contractor of the FDS.

- Further, if a user becomes aware of the publication of material that is linked to the FDS, its workers or its clients which would be deemed distasteful or inappropriate, the user should report such conduct to the FDS's Human Resources Department.

- If a user is unsure about whether they should publish material on the internet, they should seek guidance from the Computer Security officer, IT, and:

    - Include the following disclaimer example in a reasonably prominent place if they are identifying themselves as an employee of the practice on any posting: 'The views expressed in this post are mine and do not reflect the views of the practice/business/committees/boards that I am a member of', and
    - Respect copyright, privacy, fair use, financial disclosure, and other applicable laws when publishing on social media platforms.

Social media activities internally and externally of the practice must be in line with this policy.

Email/Message

Appropriate standards of civility should be used when using email and other messaging services to communicate with other staff members or any other message recipients. When using the email or messaging system users must not send:

- Angry or antagonistic messages – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures.
- Offensive, intimidating or humiliating emails – the FDS's IT resources must not be used to humiliate, intimidate, or offend another person/s based on their race, gender, or any other attribute prescribed under anti-discrimination legislation.

Guidelines for use of the FDS's email system

A user must comply with the following guidelines when using the FDS's email system:

- Any disclaimer which is automatically included in the FDS's emails must not be removed.
- If a user receives an email which they suspect contains a virus, they should not open the email or any attachment to the email and should immediately contact the IT service desk for assistance.
- If a user receives an email the content of which (including an image, text, materials, or software) is in breach of this policy or any the FDS's other policies, the user should immediately delete the email and report the matter to the computer security officer, IT. The user must not forward the email to any other person.
- Users must not publish the FDS email address on a private business card.
- Users must not forward or copy emails that contain personal information about an individual without the prior permission of that individual. They must be sent by return email to address provided.
- Patient must be advised email is not secure method of communication and noted in their clinical notes.
- Endeavor to answer emails within 2 working days or have an auto respond message.
- Users must always adhere to guidelines and prohibitions set out in this policy.
- Messaging and email must not be used for private commercial purposes except where the work is for the purposes of a corporate entity in which the FDS holds an interest.

Mobile phones and mobile devices

Mobile phones and/or mobile devices provided by the FDS to staff members, for the purposes of carrying out FDS business and accessories, and associated telephone numbers always remain the property of the FDS.

Mobile phones and mobile devices are considered IT resources and, as such, their use is governed by this policy. If mobile devices are provided the users are responsible for understanding the costs associated with using the FDS's mobile phones and mobile devices and should ensure that this equipment is used in the most cost-effective manner.

All costs associated with the use of mobile phones and mobile devices will be included in the appropriate management budget reports. Periodic checks and trend analysis will be undertaken by the IT Department on all costs associated with the use of mobile phones and mobile devices.

An investigation may be undertaken where it is identified that a user is exceeding reasonable personal use of the equipment provided.

Guidelines for use of the FDS's mobile phone and mobile devices

Users must comply with the following guidelines when using the FDS's mobile phones and mobile devices:

- Users must maintain the operational effectiveness of the mobile phone or mobile device (i.e. keeping the batteries charged when required to be contacted).
- Mobile phones and mobile devices must always be password protected and encrypted. Users are not to remove or modify such security features as configured by the IT Department.
- International and premium number call facilities will not be available without prior agreement for both business and private use and must be approved by the budget holder for the phone.
- Requests to allow international use should be made through the IT coordinator.
- Users are prohibited from using mobile phones or devices while operating a motor vehicle.
- Users must report any loss, theft, damage, or security breach of any mobile phone or mobile device immediately to the IT coordinator to ensure appropriate measures are taken to secure and disable the device. If such loss, theft, or damage is due to the negligence of the user, the user may be responsible for the cost of replacing or repairing the mobile device.

Monitoring – email, files, internet downloads or data storage

FDS does not generally monitor email, files, internet downloads or data stored on its IT resources. However, the FDS reserves the right to access and monitor any computer or other electronic device connected to the FDS's network. This includes equipment owned by FDS and personal computing equipment (for example, laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for any reason, including but not limited to, suspected breaches of this policy by a user or unlawful activities. Access to and monitoring includes, but is not limited to, email, web sites, server logs and electronic files.

FDS may keep a record of any monitoring or investigations.

PCEHR

Personally Controlled Electronic Health Record (PCEHR) Security and Access Policy

PURPOSE

To provide guidance for staff and contractors about access to, and use of, the Personally Controlled Electronic Health Record system. To provide guidance in the use of information technology in the organisation as it relates to the PCEHR system.

SCOPE OF POLICY

This policy applies to all staff (including its employees and any healthcare provider to whom the organisation supplies services under contract) with access to the Personally Controlled Electronic Health Record system.

RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE MONITORING

The following roles are responsible for implementation and compliance monitoring of the PCEHR policy:

- Responsible Officer: The RO has legal responsibility for compliance with this policy and compliance with the national PCEHR legislation.
- Organisation Maintenance Officer: The OMO is responsible for implementation and compliance monitoring of the PCEHR policy, and for maintenance of the policy.

RELATED DOCUMENTS/LINKS

This policy is to be read in conjunction with the following documents:

- https://www.myhealthrecord.gov.au/for-healthcare-professionals/my-health-record-ingeneral-practice
- PCEHR Rules 2012
- Personally Controlled Electronic Health Records Act 2012
- Personally Controlled Electronic Health Records Regulation 2012
- RACGP Computer and Information Security Standards
- Healthcare Identifier Act 2010

DEFINITIONS

- Access control mechanisms include default access controls and advanced access controls.
- Access flag means an information technology mechanism made available by the System Operator to define access to a consumer's PCEHR.
- Access list means the record associated with a consumer's PCEHR that specifies the registered healthcare provider organisations permitted to access a consumer's PCEHR.
- Act means the Personally Controlled Electronic Health Records Act 2012.

- Advanced access controls mean the access controls that enable a registered consumer to set controls on the registered healthcare provider organisations and nominated representatives who may access the consumer's PCEHR, and the records within the PCEHR.
- Consumer-entered health summary means the summary of information, including medications and allergies, that a registered consumer may enter his or her PCEHR and which is available to anyone with access to the consumer's PCEHR.
- Default access controls means the access controls that apply where a registered consumer has not set controls on the registered healthcare provider organisations or nominated representatives who may access the consumer's PCEHR.
- Document code means a code which may be used to restrict access to individual records within a consumer's PCEHR in accordance with paragraph 5(1)(c).
- Effectively remove, in relation to a record in a consumer's PCEHR, means rendering the record inaccessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer, including in the case of a serious threat in accordance with rules 6 and 7.
- Healthcare identifier has the same meaning as in section 9 of the Healthcare Identifiers Act 2010.
- Identified healthcare provider has the same meaning as in the Healthcare Identifiers Act 2010.
- Network hierarchy means a network of healthcare provider organisations created and managed in accordance with subsections 9A(3) to (7) of the Healthcare Identifiers Act 2010.
- Network organisation has the same meaning as in the Healthcare Identifiers Act 2010.
- Organisation maintenance officer has the same meaning as in the Healthcare Identifiers Act 2010.
- PCEHR: Personally Controlled Electronic Health Record
- Provider portal means the portal provided by the System Operator that permits registered healthcare provider organisations to access the PCEHR system without having to use a clinical information system.
- Record code means a code which may be used to restrict access to a consumer's PCEHR in accordance with paragraph 5(1)(a).
- Responsible officer has the same meaning as in the Healthcare Identifiers Act 2010.
- Restore, in relation to a record, means making a record, which has previously been effectively removed, accessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer in accordance with any applicable access control mechanisms, including in the case of a serious threat to an individual's life, health, or safety.
- Seed organisation has the same meaning as in the Healthcare Identifiers Act 2010.
- Seed OMO: Organisation Maintenance Officer in seed organisation. Has primary responsibility for OMO roles and coordination of OMO activities in network organisations.
- Service operator has same meaning as in the Healthcare Identifiers Act 2010.
- System operator: Department of Health and Ageing
- Verified healthcare identifier means a healthcare identifier assigned to a consumer in relation to which the service operator has evidence, to the service operator's satisfaction, of the consumer's identity.

POLICY

AUTHORITY TO ACT

The RO and OMO for this seed organisation are authorised to act on its behalf in dealing with the System Operator. Where there is a network hierarchy, the RO and OMO from the seed organisation and the OMO from the network organisation in the network hierarchy are authorised to act on behalf of the organisation in dealing with the System Operator.

ACCESS FLAGS

Where appropriate to the size and complexity of this organisation, the RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation. The network hierarchy will define the seed organisation, the network organisations that fall under that seed organisation, and the network organisations for whom access flags are appropriate.

In setting and maintaining access flags, the RO/Seed OMO will ensure that:

- Consumers can determine and control access to their eHealth records in a way that meets reasonable public expectations. Network organisations that would not be expected by consumers to be connected will thus have their own access flags.
- The organisation can share health information internally in an appropriate manner.

The RO/OMO will undertake reviews of the network structure and access flag assignments at such times as the structure changes, or in the case that a System Operator or consumer query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

MAINTAINING RECORDS OF PCEHR USE WITH THE SYSTEM OPERATOR

Where this organisation is part of a network hierarchy, the RO/OMO will establish and maintain an up-to-date record, which details the linkages between organisations in the network hierarchy, with the System Operator.

Where individual healthcare providers in the organisation are authorised to access the PCEHR system on its behalf, using the provider portal, the OMO(s) will establish and maintain an accurate and up-to-date list of individuals with the System Operator. If an individual healthcare provider is no longer authorised to access the provider portal on behalf of the organisation, the OMO will ensure the System Operator is informed and the individual removed from the list of authorised users.

ACCESS TO THE PCEHR

Organisational staff must only access the PCEHR if this access is required by the duties of their role. All staff members whose role requires them to access the PCEHR will be provided a unique user account with individual login name by the OMO. The organisation will maintain records linking user accounts to individual staff so that these can be matched in the case of an audit by the System Operator.

Staff will ensure that they assign a secure password to their user account and keep their password secret. For more information about secure passwords and maintaining user accounts, please refer to the RACGP Computer and Information Security Standards.

The administration staff can help patients with the assisted registration form and identify them according to the 3 visits and Medicare card. The doctor or nurse can do the assisted registration and upload the summary with the patient.

The RO/OMO will ensure that they immediately suspend or deactivate individual user accounts in cases where a user:

a) leaves the organisation.
b) has the security of their account compromised; or
c) has a change of duties so that they no longer require access to the PCEHR system.

User accounts will not be used by multiple staff members. All users will ensure that they log out of the system when they are not using it to prevent unauthorised access.

IDENTIFICATION OF STAFF MEMBERS WITH AUTHORISED ACCESS TO THE PCEHR SYSTEM

The OMO will maintain a record of authorised Healthcare Provider Identifier – Individual numbers in the clinical software and in the organisation's internal records. The clinical software will be used to assign and record unique internal staff member identification codes. This unique identification code will be recorded by the clinical software against any PCEHR system access.

The organisation will maintain records (e.g. staff rostering records) as to allow it to determine which user accessed the system on a particular day. These records must be maintained to allow audits to be conducted by the System Operator. Where required, the organisation will maintain staff rostering records to assist in identifying authorised users that have accessed the PCEHR system.

STAFF TRAINING

All staff with authorisation to access the PCEHR system on behalf of the organisation will be required to undertake PCEHR training. Existing staff will undertake PCEHR training before they first access the system, while new staff will be required to undertake training, if appropriate to their role, as part of their orientation to the organisation.

Staff training will provide information about how to use the organisation's clinical software, and/or the PCEHR Provider Portal, to access the eHealth record system accurately and responsibly. Staff training will consist of a combination of training materials provided by the system operator through the learning center, and training specific to the clinical software used by the organisation.

If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the PCEHR system.

The OMO will oversee a register of staff training as it relates to the PCEHR.

REPORTING SECURITY BREACHES

If any staff member becomes aware of a security breach, it is their responsibility to follow the reporting procedure outlined in the procedures section below. All breaches will be reported to the OMO/RO who will ensure that the breach is reported to the System Operator.

A security breach is when any unauthorised person accesses the PCEHR, or when a staff member with access to the PCEHR discovers that someone else may have gained access to their user account.

RESPONDING TO PATIENT COMPLAINTS

The organisation will make patients aware of the process for raising issues or complaints and will log any issues that they are made aware of. Where a patient asks the organisation to remove or amend a shared health summary or other document, and the medical practitioner agrees, the request will be logged with the organisation's OMO, and the document removed within 7 days.

In cases where there is disagreement between the medical practitioner and the patient about amendments to a shared health summary, the patient will be made aware of the ability to lodge a complaint with the Office of the Information Commissioner.

MAINTAINING ORGANISATION'S PCEHR POLICY

The OMO is responsible for ensuring the accuracy of the organisation's PCEHR policy and its compliance with PCEHR legislation. The OMO will ensure that the policy remains current and reflects changes in PCEHR legislation and in the structure of the organisation.

ACCESS TO THE PCEHR POLICY

The OMO/RO will ensure that a copy of the organisation's PCEHR policy is made available to the System Operator within 7 days of receiving the request where this request has been made in writing. The OMO/RO will ensure that the version of the PCEHR policy provided is the version of the organisation's policy that was in force on the dates specified by the System Operator in its written request.

RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE MONITORING

The following roles are responsible for implementation and compliance monitoring of the PCEHR policy:

- Responsible Officer: The RO has legal responsibility for compliance with this policy and compliance with the national PCEHR legislation.
- Organisation Maintenance Officer: The OMO is responsible for implementation and compliance monitoring of the PCEHR policy, and for maintenance of the policy.

PROCEDURES

ACCESS FLAGS

The RO/OMO will refer to review 'Section B' of the Registration booklet for healthcare organisations to determine whether the organisation has a simple or complex organisational structure. Where the

RO/OMO determines that a complex organisational structure applies, they will ensure that the understand access flags and network hierarchies before applying to the Health Identifier service and assigning access flags.

Where a complex organisational structure applies, and where a patient raises concerns about the ability to control access to their eHealth record within the organisational structure, the RO/OMO will ensure that a review of the network hierarchy and the assignment of access flags is undertaken.

MAINTAINING RECORDS OF PCEHR USE WITH THE SYSTEM OPERATOR

The OMO will determine whether the practice management software keeps a record of the individual staff members assigned to a particular user account. If not, the OMO will create and maintain a separate record which details the links between user accounts and individual staff.

Where individual health providers are authorised by the organisation to access the PCEHR Provider Portal, the OMO will maintain the currency of this authorisation by adding new staff and removing any staff who no longer require access to the PCEHR or leave the organisation.

REPORTING SECURITY BREACHES

If any staff member becomes aware that their user account has become compromised or that someone has used their computer to gain unauthorised access to the PCEHR, they are to immediately inform the OMO/RO. If only the OMO is informed, it is the OMO's responsibility to ensure that the RO is made aware of the issue.

The RO/OMO will create a log entry of the breach including details of the date and time of the breach, the user account that was involved in the unauthorised access, and which patient's information was accessed (where known).

The RO/OMO will also undertake appropriate mitigation strategies, including, but not limited to:

- Suspending/deactivating the user account
- Changing the password information for the account
- Reporting the breach to the System Operator

MAINTAINING ORGANISATION'S PCEHR POLICY

As part of their responsibility for maintaining the organisation's PCEHR policy, the OMO will ensure that:

- The PCEHR policy has a version number.
- Each time the policy is updated, the new version contains a unique version number and the date when that iteration came into effect.
- The policy is reviewed at least annually.
- The policy is reviewed at any time that changes to the PCEHR system occur, or when changed risks are identified.
- The review should examine:
    - Any potential security risks that may result in PCEHR records being accessed by unauthorised users.

- Any changes to the PCEHR system that may affect the healthcare provider organisation.
- Any relevant legal or regulatory changes that have occurred since the last review.

The OMO will ensure that copies are kept of each version of the PCEHR policy.
Policy Manager Goran Mujkic

REVISION HISTORY (to be maintained by Organisational Maintenance Officer).

BREACH OF THIS POLICY

Where the FDS's or finds evidence of a breach of this policy, FDS reserves the right to restrict a user's access to its IT resources.

Any user found to have violated this policy may be subject to disciplinary action.

Criminal offences will be reported to the police.

Data Breach

Practice Data Breach Response Plan

Procedure

1. This Data Breach Response Plan (Response Plan) sets out the procedure to be followed by Deloraine & Westbury Medical Pty Ltd staff if the practice experiences a data breach or suspects that a data breach has occurred.

2. A data breach occurs when personal information (defined in section 6 of the Privacy Act 1988 (Cth) is lost or subjected to unauthorized access, modification, use or disclosure or other misuse. Personal information refers to information that identifies or reasonably identifies an individual.

3. A data breach will also occur where protected practice information is unlawfully used or disclosed. 'Protected D & WMC information' includes a broader range of information than "personal information" as it includes information about all entities, not just medical notes.

4. Examples of a data breach include when:
   - A data base containing medical records is hacked.
   - Health information is mistakenly provided to the wrong person.
   - A device containing patients' medical records is lost or stolen

5. Whilst the process outlined in this Response Plan applies to all data breaches it is important to note that in some instance, the privacy provision may impose stricter standards on the Practice than those contained in this Response Plan. Thus, where a breach involves 'protected Practice information' both the Response Plan and the legislation must be considered collectively.

6. It is also important to note that Office of the Australian Information Commissioner (OAIC) is only concerned with breaches that involve personal information. Data breaches that involve 'protected Practice information' that is not 'personal information' do not need to be reported to the OAIC.

7. Adherence with the Response Plan will ensure that the Practice can contain, assess, and respond to data breaches in a timely fashion to mitigate potential harm to affected persons.

8. This plan:
   - Sets out the roles and responsibilities of staff.
   - Sets out the contact details of appropriate staff in the event of a data breach; and
   - Outlines the procedure to be followed in the event of a data breach.

The Practice Staff member to notify the practice manager

9. Immediately notify the practice manager of the suspected data breach.

10. Record and advise the practice manager of the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.

Practice Manager to assess the breach

11. The practice manager must assess and determine whether a data breach has occurred.

12. If the practice manager has any suspicion that a breach has occurred, the practice manager must immediately notify the CEO and Medical Director of the Practice.

Practice Manager and CEO/Medical Director to assess the seriousness of the breach

13. In some instances, a minor breach may be able to be dealt with at the practice level. Where a minor breach is dealt with at the director level, the following details must be recorded:
    - Description of the breach or suspected breach.
    - Action taken by the practice manager to address the breach or suspected breach.
    - Outcome of that action
    - Sign off from the CEO/Medical Director that no further action is required; and
    - Confirmation that the incident has been recorded in the practice Data breach incident log.

14. The record must be saved in the folder below:
    - Data breach register in office
    - Practice managers C:\ drive

15. If the breach is serious, it must immediately be escalated to the practice Manager and the CEO/Medical Director who will then determine whether the directors of the Practice are involved.

Data Breach Response Team

16. The Response Team includes:
    - Practice: Goran Mujkic CEO – 0408 433 980
    - Legal: Practice indemnity MDA National – 1800 011 255
    - IT: Another Computer Store – Toby 6344 4423 or 0499 030 766

17. It is not necessary that all members of the Response Team be included in all data breach responses. The practice manager will determine whether the Response Team is to be advised.

Process:

18. Once a matter has been escalated to the Response Team, the process outlined below must be followed. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances.

19. There are four key steps to consider when responding to a breach or suspected breach. Generally, steps 1-3 should be carried our concurrently or in close succession.
    - Step 1: Contain the breach and or conduct a preliminary assessment.
    - Step 2: Evaluate the risks associated with the breach.
    - Step 3: Notification.
    - Step 4: Prevent and protect from future breaches.

Step 1: Contain the Breach and do a preliminary assessment

Contain the breach

20. Once a data breach has been identified, action must be taken to immediately contain it. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached.

Initiate a preliminary assessment

21. Move quickly to appoint someone to lead the initial investigation. This person must be suitably qualified and have sufficient authority to conduct the initial investigation. In some instances, this may be a member of the Response Team. In other instance, it will be a person most suitably qualified to carry out the initial investigation (as determined by the members of the Response Team).

22. In some situations, it will be necessary to assemble a team that includes representatives from appropriate areas of the practice to conduct the preliminary assessment.

23. The following questions should be addressed when making the preliminary assessment:
    - What information does the breach involve?
    - What was the cause of the breach?
    - What is the extent of the breach?
    - What are the harms (to affected persons) that could potentially be caused by the breach?
    - How can the breach be contained?

Step 2: Evaluate the risks associated with the breach

24. The following factors are relevant when assessing the risk:

The type of information involved

a) Is it personal information or protected practice information?
b) Does the type of information that has been compromised create a greater risk of harm?
c) Who is affected by the breach?

Determine the context of the affected information and the breach

a) What is the context of the information involved?
b) What parties have gained unauthorized access to the affected information?
c) Have there been other breaches that could have a cumulative effect?
d) How could the information be used?

Establish the Cause and extent of the breach

a) Is there a risk of ongoing breaches or further exposure of the information?
b) Is there evidence of theft?
c) Is the information adequately encrypted, anonymized or otherwise not accessible?
d) What was the source of the breach? (risk of harm may be lower where source of the breach is accidental rather than intentional)
e) Has the information been recovered?
f) What steps have already been taken to mitigate the harm?
g) Is this a systemic problem or an isolated incident?
h) How many persons are affected by the breach?

Assess the risk of harm to the affected persons

a) Who is the recipient of the information?
b) What harm to persons could result from the breach?
c) Assess the risk of other harms
d) Other possible harms, including to the agency or organisations that suffered the breach.

For example:

- The loss of public trust in the Practice
- Reputational damage
- Legal liability
- Breach of secrecy provisions

25. A thorough evaluation of the risks will assist the Practice in determining the appropriate course of action to take.
    - If remedial action was taken and the error was not likely to result in serious harm – no eligible data breach. Therefore, no notification obligations under the legislation.

Step 3: Notification

Deciding whether to notify affected individuals or entities

26. In general, if a data breach creates a real risk of serious harm to a person, the affected person should be notified.
27. The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected person.
28. Consider the follow factors:
    - What is the risk of serious harm to the person as determined by step 2.
    - What is the ability of the person to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)?
    - Even if the person would not be able to take steps to fix the situation, is the information that has been compromised sensitive or likely to cause humiliation or embarrassment?
    - What are the legal and contractual obligations to notify and what are the consequences of notification?

Notification process

29. In general, notification should occur as soon as reasonable possible. However, in some instances, delay may be necessary.

30. Notifications should be direct – by phone, letter, email or in person, to the affected individuals.

31. Indirect notification, either by website, posted notices or media should only occur when direct notification could cause further harm, is cost prohibitive or the contact information for affected persons is unknown.

Details to include in the notification

32. The content of the notification will vary depending on the particular breach and notification method. However, the OAIC recommend that notifications should include the following information:
    - Incident description.
    - Type of information involved.
    - Response to the breach.
    - Assistance offered to the affected persons.
    - Other information sources designed to assist in protecting against identity theft or interferences with privacy (e.g. www.oaic.gov.au);
    - The practice contact details.
    - Whether breach notified to regulator or other external contact(s)
    - Legal implications (e.g. the privacy provisions);
    - How individual can lodge a complaint with the practice; and
    - How individuals can lodge a complaint with the OAIC (where the information is personal information).

Other notifications

33. It may also be appropriate to notify other third parties, such as:
    - The OAIC.
    - The Police.
    - Insurance providers.
    - Credit card companies, financial institutions.
    - Professional or other regulatory bodies.
    - Other internal or external parties who have not already been notified.
    - Agencies that have a direct relationship with the information lost/stolen.

34. The OAIC strongly encourages agencies to report serious data breaches involving personal information. The following factors should be considered in deciding whether to report a breach to the OAIC:
    - Any applicable legislation that may require notification.
    - The type of personal information involved and whether there is a real risk of serious harm arising from the breach.
    - Whether many people were affected by the breach.

- Whether the affected individual have been notified; and
- If there is a reasonable expectation that he OAIC may receive complaints/inquiries about the breach.
- GPs and their staff can seek advice from their medical defence organization if unsure how to proceed in a particular situation.

Step 4: Prevent future breaches.

35. Once immediate steps have been taken to mitigate the risks associated with a breach, the Practice must take the time to investigate the cause of the breach and protect and prevent future attempts at intrusion/breach.

36. The practice Owners/Directors must be briefed on the outcome of the investigation, including recommendations:
    - To make appropriate changes to policies and procedures if necessary.
    - Revise staff training practices if necessary; and
    - Update this Response Plan if necessary.

Server - Secure Site and Temperature Monitoring

Policy: Provide a secure site for server to meet minimum standards

Cooling

a) Sufficient for size of server and room – heat pump running on AUTO 22 degrees.
b) Temperature must be monitored and maintained between 18-24 degrees.
c) To be monitored using TADO application by Goran Mujkic / Manager.

UPS and Backup

a) Maintenance and testing by IT (Another Computer Store)
b) UPS sized to meet current and future needs with sufficient battery backup to allow for controlled shutdown.

Access Control

a) Door to always remain locked.