AHPRA

Aboriginal and Torres Strait Islander Health Practice
Chinese Medicine
Chiropractic
Dental
Medical
Medical Radiation Practice
Nursing and Midwifery

Occupational Therapy
Optometry
Osteopathy
Pharmacy
Physiotherapy
Podiatry
Psychology

Australian Health Practitioner Regulation Agency

Information and IT Acceptable Use Policy – Board and Committee Members IS010

August 2018

Purpose and scope

Purpose

The purpose of this policy is to specify and promote responsible and appropriate use of protected information and information technology (IT) facilities managed by AHPRA for the purposes of the National Registration and Accreditation Scheme (NRAS) established under the *Health Practitioner Regulation National Law* (as in force in each state and territory) (the National Law).

Protected Information is defined as information that comes to a person's knowledge in the course of, or because of, the person exercising functions under the National Law. Some of the terms used in this policy are defined in the definitions section.

Introduction

Appropriate and responsible use of protected information and IT facilities is defined as use that is consistent with the law and the objectives of the NRAS and complies with any information security governance arrangements and policies which might be agreed and implemented from time to time.

Scope

The policy applies to board, committee and panel members who use or have access to AHPRA IT facilities (including iPads) and protected information. Other AHPRA users such as staff and contractors should refer to the Information and IT Acceptable Use Policy – Staff – IS002.

Policy

Key areas

1. There are 5 key areas that underpin this policy. The table below outlines a high level policy statement for each. Further details are provided in the following sections.

Key area	Guiding principle
Handling protected information	You have the responsibility to use, hold and disclose protected information including sensitive information in accordance with the National Law, Commonwealth Privacy Act and AHPRA's corporate policies referred in the 'Related Policies' section below.
AHPRA issued iPad and IT facilities	IT systems and facilities must primarily be used for the purposes of NRAS and in the interests of performing your duties under the terms of your board, committee or panel appointment.
Using the internet via AHPRA Wi-Fi or SIM card	The internet must be used responsibly and productively. Limited personal use is permitted.
Using email	Board members with AHPRA email addresses must use the official email to perform their NRAS duties. Email must be used in line with

	the expectations outlined in this policy and other relevant AHPRA corporate policies referred in ‘Related documents’ section below.
Monitoring	AHPRA has the ability and authority to monitor and track activities on AHPRA-issued iPads and may monitor use to ensure compliance with this and related policies.

Policy applicable to all users

Handling protected information

2. Everyone handles protected information when performing their regulatory functions under the NRAS and has a responsibility to keep that information secure and use it properly.

3. When handling protected information you are responsible for:

    3.1. conducting yourself in accordance with the National Law, AHPRA Information Security Policy, AHPRA Privacy Policy and the Privacy Act

    3.2. taking due diligence and due care to secure data, documents and protected information you obtain in the course of your duties

    3.3. complying with the security mechanisms built into IT equipment and not attempting to circumvent security controls

    3.4. securing the login credentials allocated to you and being accountable for activities performed under your login. You must choose strong passwords and not disclose or share passwords or other authentication material.

    3.5. not disclosing user or practitioner personal information obtained through your regulatory role to anyone for other than for the designated regulatory purposes. Not using AHPRA IT facilities to improperly store or process information that could result in legal action against AHPRA or yourself.

    3.6. not disclosing any protected information in the public domain. Refrain from accessing or communicating personal or protected information in public locations (e.g. public transport, transit lounges and coffee shops) unless extra care is taken to minimise the chance of being overheard or having the screen of any device observed, also called shoulder surfing.

    3.7. being aware of social engineering and exercise caution. You should be aware of methods used by scammers and fraudsters to gain information. Some methods include calling and impersonating AHPRA or Telstra staff, then requesting user names and passwords. Be aware that legitimate organisations will never request these details.

    3.8. ensuring protected information is not used for commercial gain, advertising, sponsorship, placing a third party in a position of commercial advantage or resulting in material loss to AHPRA or the boards.

    3.9. Restricted, confidential or sensitive AHPRA and board information (such as any information you obtain in the course of your duties) **must not** be shared or transmitted, except when this is necessary to perform functions under the National Law. In particular, users **must not** store information obtained for the purposes of the National Law on third party, cloud-based services such as iCloud, Dropbox or Evernote or transfer this information to an unauthorised device. Board documents must not be emailed to non-AHPRA email accounts, unless adequately password protected and in accordance with arrangements for which you have gained written approval. Such arrangements might be agreed upon from time to time.

    3.10. Privacy breaches must be promptly reported to the Serious Incident Hotline either by email riskmanagement@ahpra.gov.au or by telephone on (03) 8708 9331.

AHPRA issued iPads and IT facilities

4. AHPRA issued iPads should be used primarily for business purposes and in the interests of serving the objectives of the NRAS. iPads may be used for limited personal or business use as long as this use does

not hinder its principal use for AHPRA or board/panel/committee business. All use must be lawful and consistent with applicable AHPRA policies.

5. iPads remain AHPRA's property and must be returned on request and/or at the completion of the appointment to boards, panels or committees

6. You must not permit another person to use or access your AHPRA issued iPad, unless that other person is authorised by AHPRA to do so.

7. You must use the AHPRA issued iPad lawfully and ethically. The iPad is to be used like any other business resource and you must comply with any laws, policies, and codes of conduct or legislative requirements which apply. Where required by law or if AHPRA reasonably suspects unlawful activity may have occurred, inappropriate or illegal use may be reported to authorities.

8. You are expected to limit downloads on 4G to business use. This service is provided to facilitate access to AHPRA and board/panel/committee information.

9. You must exercise due care of the AHPRA issue iPad. This includes, dropping or placing heavy objects (book, laptops, etc) on the iPad, using a protective case/covers for the iPad, as provided by AHPRA, not subjecting the iPad to extreme temperatures, and not storing or leaving the iPad unattended in a vehicle.

10. Board and committee members may use their own devices to access Diligent Boards or PowerBI as well as or instead of their AHPRA iPad. AHPRA will assist with support and maintenance issues regarding the supplied iPad but will not support or subsidise the cost of other devices or data access.

Using AHPRA's internet connection

11. Use of the AHPRA internet via Wi-Fi or 4G is permitted and encouraged where it supports the goals and objectives of the NRAS.

12. Web content filtering has been implemented on AHPRA Wi-Fi to prevent inappropriate and non-business related content and minimise the risk of a security breach, so users may find some websites blocked.

13. AHPRA logs the internet use of all users. These logs can be used for optimising web content filtering policy and investigating reported or suspected misuse.

14. You must not upload or store private, sensitive or confidential corporate data in public cloud systems, including but not limited to online data storage sites, document exchange web sites, or personal email accounts.

15. International data roaming is disabled in iPads.

Using your AHPRA email account (National Board Chairs only)

16. When using an AHPRA email account, it is your responsibility to:

    16.1. respect the intended business use of email exchange and usage shall not be in breach of the relevant policies referred in 'Related documents' section below

    16.2. report suspected phishing/hoax emails to the Service Desk for further investigation

    16.3. be cautious while opening/viewing emails from unknown or suspicious senders. Do not open web links or open attachments in SPAM emails. In Outlook click 'Block Sender' to automatically mark email as Junk and move into the 'Junk E-mail' folder.

    16.4. only send emails to practitioners or members of the public for the purpose of performing your AHPRA duties

    16.5. avoid emailing protected information of a sensitive, private or confidential nature to external parties however, if this is unavoidable, ensure that the addressee is correct and that the data is properly protected

    16.6. note that email attachment size is limited to a maximum of 10 MB per email

16.7. refrain from using your AHPRA email in internet forums or for registering in websites not related to your AHPRA duties. This may render email accounts vulnerable to SPAM and phishing attacks, and

16.8. when accessing AHPRA webmail from internet and public systems, you must ensure you do not leave copies of attachments with sensitive, private or confidential information in public computers and delete any copies after use.

Monitoring

17. AHPRA may undertake appropriate technical monitoring, recording and auditing of usage of protected information and IT systems as required to comply with legal, technical and policy requirements.

18. If at any time there is a reasonable suspicion that AHPRA systems are being used in breach of this policy, Board Chairs or the Executive Director, Strategy and Policy may request that your activities be electronically monitored and activity logs are used for investigation. This will be performed in compliance with legal and regulatory requirements and in compliance with any relevant board policies and guidelines.

Reporting security issues

19. You are responsible to report any policy breaches, accidental loss or suspicious use of your access credentials, loss or theft of device, loss of data, security risks and threats via information.security@ahpra.gov.au.

Policy feedback

20. If you have any queries or comments about the policy please send an email to information.security@ahpra.gov.au and your email will be responded within three business days.

Related documents

- Board Member Code of Conduct
- Privacy Policy
- AHPRA iPads: conditions of use
- Any relevant board policies and guidelines

Definitions

Term	Definition
Protected Information	Information that comes to a user’s knowledge in the course of, or because of, the person exercising functions under the National Law.
IT Facilities	IT facilities include, but are not limited to: • Hardware, such as iPads, • Software, such as dedicated applications (eg Diligent Boards, PowerBI, Airwatch), and • IT Services, such as internet and email.
Access Cards	Proximity ID / access cards provided to each member that allow them access to the AHPRA premises.
SPAM	SPAM is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.
Phishing	Phishing is the act of attempting to acquire protected information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

BYO Device	An electronic device a user supplies themselves, rather than a device issued to the user by AHPRA.
Shoulder surfing	The action of someone looking over your shoulder to gather information from the document or a screen that you are working on.
Sensitive information	Sensitive information is defined by the Australian Privacy Principles. It is a type of personal information and includes information about an individual's: • health (including predictive genetic information) • racial or ethnic origin • political opinions • membership of a political association, professional or trade association or trade union • religious beliefs or affiliations • philosophical beliefs • sexual orientation or practices • criminal record • biometric information that is to be used for certain purposes • biometric templates.

Document control

Approver	National Executive
Policy Number	IS010, Version 1.2
Date Approved	23 July 2018
Date Commenced	August 2018
Date for Review	August 2021
Policy Sponsor	Executive Director, Business Services
Sections modified	Addition of section 11 Changes to requirements for Diligent Boards software Transfer to new template Grammatical and stylistic corrections