Staff Privacy Guide

At AHPRA, protecting the privacy and confidentiality of the personal information of our staff, registrants and suppliers is very important to us. Equally, obtaining and maintaining the trust of staff, clients and our suppliers is fundamental to the way we do business.

Purpose of this Guide

The purpose of this guide is to create an AHPRA-wide awareness and understanding of our privacy obligations and to ensure that our business meets those obligations.

Background

AHPRA handles large volumes of personal information on a daily basis. We recognise we have a responsibility to treat personal information entrusted to us with respect. We recognise the sensitivity of client information we hold, and are committed to protecting its confidentiality. We recognise our legislative obligations and take steps to comply with them.

The following information relates to aspects of privacy most relevant to staff functions in gathering personal information and its appropriate use. This guide is to assist you in applying the AHPRA Privacy Policy and in doing so, to ensure that we do not contravene our legislative obligations.

For more information, please refer to the following documents:

- AHPRA Privacy Policy (423 KB, PDF)
- AHPRA Privacy Statement (306 KB, PDF)
- AHPRA HR Confidentiality Policy (198 KB, PDF)
- AHPRA Staff Confidentiality Agreement (193 KB, PDF)

Collection of Personal Information and Consent

The information AHPRA collects about individuals relates to our core functions dealing with Registration and Notifications. These core functions require us to gather names, addresses, gender, contact details and also more specific information, such as credit card numbers, bank account details and criminal history information. It is of utmost importance that staff dealing with this information use extra care to ensure that a person’s personal information is protected and only disclosed for the purpose it was collected. Use or disclosure of the personal information beyond these express purposes is prohibited, unless the use or disclosure would have been within the reasonable expectation of the person providing the information.

The disclosure rules mean that you must be very careful when giving out information about our clients, especially over the telephone. You should, as far as it is practical, establish that the person asking you for the personal information is someone who is actually entitled to receive it. If you still have doubts about disclosing the information, ask the enquirer to put their request in writing.
Dos and Don’ts

Do make sure that personal information is only used for the purpose for which it was given to us, or in the other permitted circumstances

Do check with your supervisor if someone other than the individual asks you for personal information (such as the police, hospital, government agency or a solicitor).

Do access client files only if you need to do so for your work.

Do ensure that when returning documents to clients you check that only relevant documents are returned

Don’t gossip with anyone, even your colleagues, about client information which you discover in the ordinary course of your job.

Don’t disclose personal information to external organisations or people unless you have the individual’s consent, or one of the exceptions applies, and you have your supervisor’s approval.

When Collecting Personal Information – Be Up-Front

• You must only collect information by lawful and fair means, and not in an intrusive or unreasonable way;
• You must take reasonable steps to let the client know the following:
  - That you work for AHPRA
  - Why the information is being collected;
  - What people or organisations we may pass the information on to; and
  - The fact that the individual is able to access the information we hold about them.

Sensitive Information – Be Very Careful

The Privacy Act 1988 (Cth) and the Australian Privacy Principles under the Act require sensitive information to be treated differently from other types of personal information.

Sensitive Information is information or opinion about an individual’s:

• Racial or ethnic origin; or
• Political opinions; or
• Membership of a political association; or
• Religious beliefs or affiliations; or
• Philosophical beliefs; or
• Membership of a trade union; or
• Membership a professional or trade association; or
• Sexual orientation or practices; or
• Criminal record; or
  • Health information about an individual; or
  • Genetic information about an individual that is not otherwise health information; or
• Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
• Biometric templates

What are the rules for collecting sensitive information?

Generally, sensitive information can only be collected, used or disclosed with the express consent of the individual concerned. There are only a few situations where we can collect, use or disclose sensitive information without the person’s express consent, such as where:

• We have to prevent a life threatening situation and the person can’t physically communicate consent to collection, use or disclosure, or is not legally or physically able to consent;
• We must collect the information because of legal proceedings in which we are or may need to be involved;
• If there is a serious and imminent threat to that person’s life, health or safety;
• We are required to do so by law, such as considering an applicant’s criminal history in deciding an application for registration.

The key difference between personal information and sensitive information is that we require express consent to use and disclose sensitive information, and the exceptions to this rule are much narrower. Therefore, if you do not have the consent of the person concerned to use and disclose the information, you should speak with your supervisor about whether to use or disclose the information for that purpose.

Dos and Don’ts

Don’t as a general rule, request, collect use or disclose sensitive information about a person without his or her consent.

Data Security

AHPRA is committed to ensuring that personal information is held securely. To the extent required by the Privacy Act, we will take reasonable steps to:

• Ensure that any personal information we collect, use and discloses is accurate, complete and up to date;
• Protect the personal information that we hold from misuse, loss, unauthorised access, modification or disclosure; and,
• Destroy or permanently de-identify personal information that is no longer needed for any purpose that is permitted by the Act.

AHPRA uses a wide range of physical security controls to ensure that only appropriate people gain access to our work sites, such as key cards for restricting access and the use of visitor registers.

AHPRA requires all staff to store paperwork in desk drawers, files etc when they leave for the day. Generally, all cabinets and offices should be locked after hours – especially where your work area may capture sensitive information.

AHPRA controls access to our computer systems through the use of passwords, as well as restricting what staff can do within the system (some staff may be able to modify, where others may only be able to view, the information).

Dos and Don’ts
Do make sure you completely log out of system databases when finished.

Do check with your supervisor before destroying any records that contain personal information.

Use of Email and the Internet at Work

Key Points

Read, understand and apply the principles and expected standards of behaviour described in AHPRA Information Technology Acceptable Use Policy.

It is important you read this policy because you should understand that AHPRA has a responsibility and the right to monitor employee use of AHPRA’s email and Internet facilities.

Dos and Don’ts

Do read the Information Technology Acceptable Use Policy.

Do realise that AHPRA’s computer resources are provided to you for business purposes.

Do understand that when an email is sent, a copy may be stored on any number of computers, in addition to the computer of the person who received or sent the email.

Do ensure that you use AHPRA’s computer systems in a professional, ethical and lawful manner.

Do realise that AHPRA may monitor material created, stored, sent or received via the AHPRA computer network, including personal information residing on AHPRA systems.

Don’t assume that anything you create, store, send or receive on our computer system will not be seen by anyone else.

Videoing and/or Recording Someone

Privacy laws and AHPRA’s Privacy Policy not only cover written information about a person, they also cover information collected about a person such as video and audio recordings.

Reasons why AHPRA may monitor video footage or record conversations could include:

- For security reasons
- To provide a record in the event of a dispute about the transaction
- To improve customer service, for example, monitoring training or coaching of staff who handle telephone calls.

Privacy Laws and AHPRA’s Privacy Policy generally apply to the collection of this type of personal information. For example, when AHPRA undertakes surveillance at our premises for security purposes the CCTV monitor should generally be in clear view of the public so that people are informed that “personal information” (their video image) is being collected in this way.

Monitoring (listening in to), or recording of telephone conversations, is a matter tightly controlled by law. The Federal Telecommunications (Interception) Act 1979 and State and Territory listening devices laws may both apply to this activity. The general rule is that the call may not be recorded. There are exceptions to these rules in very limited circumstances including where a warrant applies.

If a call is to be recorded or monitored, AHPRA must tell the other party at the beginning of the conversation so that the other party has the chance either to end the call, or to ask to be transferred to another line where monitoring or recording does not take place if this is available.
**Dos and Don’ts**

**Do** recognise that collection of video or audio information about individuals is limited by the Privacy Act, AHPRA’s Privacy Policy and State and Federal Acts.

**Criminal History Information**

Applicants for registration are subject to criminal history checks. This means AHPRA may collect sensitive information about applicants’ criminal history. Under the National Law, criminal history includes:

- Every conviction for an offence, and
- Every plea of guilty or finding of guilt by a court, and
- Every charge made against the person for an offence in Australia, elsewhere and whether before or after the commencement of the National Law.

**Criminal History Checks for Staff or Contractors**

Some persons dealing with AHPRA may have convictions which are spent. A spent conviction is a conviction which is not required to be disclosed, and may not be considered according to a law in the jurisdiction in which the conviction is recorded. Persons who have spent convictions include applicants for employment at AHPRA, contractors and suppliers.

The spent convictions laws, and the exemptions under the laws, vary in each state and territory.

**Key Points**

If you are unsure, you must check with your supervisor whether any questions about convictions or any use of conviction information is in accordance with the law and with our recruitment policies.

**Conclusion**

Collection of personal information is necessary for AHPRA to do its business. It is also governed by the Privacy Act which applies to AHPRA. It is essential to get it right, and there are potential penalties for failing to comply with the Act. Furthermore, people’s lives can be adversely affected by breaches of their privacy and mishandling of their personal information.

The reason for collecting personal information affects how the personal information may be subsequently used or disclosed. As a general rule, personal information should only be used or disclosed for the primary purpose for which it was collected.

**Use and disclosure of personal information** and AHPRA’s business is inexorably linked. Make Privacy top of mind in your work practices.

**Contact**

Senior FOI and Privacy Officer – Victorian and National Office: Bryan Sketchley

Email: bryan.sketchley@ahpra.gov.au

Phone: (03) 8708 9151

Contact the Privacy Officer if you have any questions or issues relating to AHPRA’s privacy policies and procedures.