

Overview of Australian Privacy Principles and Privacy Policy of Dr Day

On the 12 March 2014, 13 Australian Privacy Principles (APPs) amended the *Privacy Act 1988*. This is legislation that defines how organizations (including health service providers) deal with protection of personal health information that is collected, stored and used. The legislation is designed to promote greater openness between health service providers and consumers regarding the handling of health information.

Personal information about you, your family and related persons includes data such as your:

- name
- address
- gender
- date of birth
- contact details
- health insurance status
- GP referral details
- Appointment times

This information may be communicated to you by our practice via standard telephone, email or SMS, unless you advise us otherwise.

Sensitive information or Personal Health information (PHI) on the other hand requires strict confidentiality and the APP's apply specifically to this type of information collected from you. This includes, but is not limited to your medical information, consultations, investigations, operations, reports etc. This information will be communicated to you in person, via post or by password protected email. Communication sensitive information between health care providers is also done by secure password protected or using other secure technologies.

Australian Privacy Principle 1 — open and transparent management of personal information

The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

The information on this sheet is Dr Day's privacy policy.

Australian Privacy Principle 2 — anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

Anonymous service: While the legislation allows for you to adopt an alias identity if desired, this is not recommended and it severely limits your access to hospitals, other health providers, insurance refunds and the provision of appropriate health care. Dr. Day may not be able to provide a service to you under these circumstances, as it is not practicable. Further more, provision of some services are illegal if you are not identified correctly, e.g. provision of a prescription, notification of notifiable diseases etc.

Australian Privacy Principle 3 — collection of solicited personal information

This includes both personal and sensitive information

Collection of information: Where possible, most information is collected directly from you. Some information about you and your health may be collected from your GP, other medical practitioners, or from other health professionals. Only information relevant to providing a health service and the necessary associated administrative functions is collected. The collection of information is performed only by employed members of Dr Day's Practice and is collected in a confidential manner. A private interview room is available to convey sensitive information to and from patients when required. Consultations with Dr Day are confidential.

Australian Privacy Principle 4 — dealing with unsolicited personal information

Policy: This type of information will only be kept securely on your file if it is relevant to your health care provided by Dr Day. If not it will be destroyed.

Australian Privacy Principle 5 — notification of the collection of personal information

Privacy consent: As a patient of this practice you need to be aware of our policy and you will be asked to sign (initial) that you have read this policy and have understood it, prior to us collecting sensitive health information from you.

Australian Privacy Principle 6 — use or disclosure of personal information

Use and Disclosure: Information collected from you is to enable Dr Day and the clinic staff to plan, coordinate and implement appropriate health care. This may involve disclosure to other health professionals, for example an anaesthetist, specialist nurse, dietitian, physiotherapist, pathologist, radiologist or any other health professional involved in the provision of your care. Information is not handed on to commercial bodies unrelated to the provision of your health service, such as the media, fund-raising bodies or direct marketing. The legislation defines that reasonable expectations for disclosure include organizations associated with: (but not limited to) billing or debt recovery, government health departments, medical experts, lawyers acting for legal proceedings, conditions requiring notification to government bodies, clinical audit and quality control programs. De-identified data may be submitted to national audit bodies for quality control of professional standards.

Disclosure can also occur to a "responsible person" in order to provide appropriate care or on compassionate grounds. For example, telling a parent, child, defacto, guardian, or nominated person the results of surgery or prognosis following an accident may occur. Where disclosure is requested from a third party, e.g. an insurance company, you must supply written consent expressly naming the body to which disclosure is to occur.

Australian Privacy Principle 7 — direct marketing

Direct marketing: We do not use or disclose your information for the purpose of direct marketing.

Australian Privacy Principle 8 — cross-border disclosure of personal information

Trans-border flow on information: No information is transferred about you to overseas destinations, unless you provide an overseas address as your contact address, or you provide details to us of health providers involved in your care which are based overseas.

Australian Privacy Principle 9 — adoption, use or disclosure of government related identifiers

Identifiers: This practice identifies your personal electronic medical record by using a specific unit record number.

Australian Privacy Principle 10 — quality of personal information

Data Quality: While every effort is made to ensure data is accurate, up to date and relevant at the time of initial collection, once you are no longer an active patient of this practice, no further checking of data quality is performed. You may request to view your record if you feel that data quality is not accurate.

Australian Privacy Principle 11 — security of personal information

Data Security: This practice keeps all data on an electronic record securely kept on password computers held on this practice and on password protected laptop computers. Only practice employees have access to the data, (all practice employees are health related personnel). Archived records are kept in a secure locked location on and off site. Medical record information is not accessible via the World Wide Web. Medical records may be kept indefinitely for medico-legal reasons. Some additional data may also be secured stored on paper records.

Australian Privacy Principle 12 — access to personal information

Request for access: Access and correction to your information can be made by you but only after you have been positively identified. This usually is by personal attendance at the practice to ensure your information is not given to anyone else claiming on your behalf. A simple request, such as the result of a test can be provided at the time of consultation after verbal request. Requests for more complex matters, or for the medical record need to be in writing. Such request will be processed in 30 days and attract an administration fee on provision of the information to the individual of \$65. Access can be denied where specific legislation prohibits such action for example, where the disclosure poses a serious threat to the life of the individual, privacy of other individuals may be affected or the request is frivolous.

Australian Privacy Principle 13 — correction of personal information

Correction: Amendments to an incorrect record can be noted and included in the medical record, but for medico-legal reasons, the original medical record cannot be erased, modified or altered.