



GP GUIDE TO THE PRIVACY AMENDMENT (PRIVATE SECTOR) ACT 2000 AND THE NATIONAL PRIVACY PRINCIPLES (NPPs)

Background - Privacy Act 1988 and Privacy Amendment (Private Sector) Act 2000

The new privacy laws give individuals the right to access any personal information an organisation holds about them, the right to correct that information if it is inaccurate, the right to complain if they think an organisation has breached their privacy rights and the opportunity for redress if the breach is proven. It is important to remember that a GPs written opinions on the patient forms part of the health record and the patient will have right of access to these opinions. Right of access *does not* equate to right of ownership. Both the Act and the Amendment Act will apply to all health service providers in the private sector. The Act will protect personal and sensitive information through the National Privacy Principles or similar codes approved by the Federal Privacy Commissioner. This protection is backed by strong enforcement mechanisms. Because health providers already practice within a framework that recognises the importance of keeping individual health information confidential, many requirements under the new legislation will be familiar and will in fact reinforce what is already current practice.

Exemptions

Exemptions only exist for organisations with an annual turnover of under \$3 million p.a. that DO NOT provide a health service or hold health records, and that do not collect or disclose personal information about an individual for a benefit, service or advantage.

Employee records

The Privacy Act *does not apply* to information held by an employer about its current and former employees where that information is held in employee records and relates to the employment relationship. The Act *does apply* to information held about applicants for employment who were unsuccessful and who never entered into an employee relationship with the organisation. The Act also applies to the records of employees of other organisations when health service providers handle them, such as in relation to workers' compensation claims.

Outsourcing and Contractual Arrangements

It is essential that all future outsourcing and contractual arrangements with third parties adequately address the National Privacy Principles.

Health Providers that Operate in both Public and Private Sectors

General Practitioners may work in both the public and private hospital systems. There are also situations where, for the purposes of handling health data, it may be difficult to distinguish between services provided by the public and private sectors (eg: hospitals where public and private services are co-located). Also, initiatives such as co-ordinated care projects often involve collaboration between organisations from both public and private sectors.

As this legislation applies to the private sector only, and slightly different standards may apply in the public sector, it is important to try to distinguish between activities conducted by public and private sector organisations where possible. In situations where this is not straight forward, it is suggested the following criteria be used as a guide:

- Adhere to the standards in the NPPs where no higher privacy standards apply.
- In situations where different privacy laws apply, then apply the standard that provides the individual with the greater level of privacy protection.
- Have clear contractual arrangements regarding what privacy laws are applicable to a particular project or activity.

Hospitals and private practitioners may need to include privacy provisions in any agreements they enter into when private patients are treated in public hospitals. The agreement should clarify the parties' responsibilities for handling and storing health information.

Example - Doctor treats a private patient in a public hospital

Health information collected by a surgeon in this situation would be subject to the Privacy Act, regardless of where it is stored, because the surgeon is working in his or her capacity as a private sector health provider. However, if a hospital employs or contracts a private health provider, then the provider is subject to public sector privacy standards. The records kept by the hospital will most likely be subject to State privacy laws where these apply. In this situation, the surgeon would need to be satisfied that the information stored by the hospital was appropriately safeguarded. If the individual requests access to his or her records, the surgeon and the hospital would need to provide access to the records.

Health Information held before the Commencement of the Privacy Act

All of the new provisions in the Privacy Act are effective from 21 December 2001. Only some of the National Privacy Principles (NPPs) apply to information collected *before* 21 December 2001. These include:

- NPP 4 - Data Security;
- NPP 5 - Openness;
- NPP 7 - Identifiers;
- NPP 8 - Anonymity; and
- NPP 6 - Access and Correction (only where information is still being used or disclosed and providing access would not pose an unreasonable administrative burden or expense on the GP).

SUMMARY OF THE NATIONAL PRIVACY PRINCIPLES

NPP 1 - Collection

An organisation must not collect information unless it is necessary for one or more of its functions or activities. Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, how the person can get access to their personal information and what happens if the person does not give the information. Where possible, information should be collected directly from an individual and not a third party. If information is collected from a third party, the individual should be told as soon as practical what information has been collected, by whom, for what purpose and how it may be accessed.

- *Note: Some of this information may overlap with that relating to NPP 5. The difference is that an organisation is obliged to make an individual aware of the above. Information that relates to NPP 5 only needs to be made available if it is requested.*

NPP 2 - Use & Disclosure

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

- This provision *does not* prevent a GP from disclosing health information about an individual to someone else if: the second person is *responsible* for the individual or the GP is satisfied disclosure is necessary for appropriate care or disclosure is not contrary to the wishes of the individual. However, individuals should be aware of, and consent to, the disclosure of information to other health care providers, including referrals to specialists and hospitals.
- Consent is required when health information is used for research or statistical purposes or for any purpose other than that for which it was collected.
- This provision will have a major impact on what happens to patient information when a surgery undergoes a change in business circumstances or closes. Refer to Alliance Information Sheet 3 for more information.
- *Note: A person is *responsible* for an individual if they are a parent, a child or sibling aged at least 18 years, a spouse or de facto spouse, an immediate relative aged at least 18 years that is also a member of the individual's household, a guardian or have power of attorney that is exercisable in relation to the individual's health, have an intimate personal relationship with the individual or have been nominated by the individual in case of an emergency.*

NPP 3 - Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to date.

NPP 4 - Data Security

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

- This is a particularly sensitive issue for GPs. All health records need to be adequately protected from theft, loss, unauthorised alteration, unauthorised distribution etc. Paper based records should be stored in a lockable environment. Electronic health records (including data stored on a back-up medium) should be equally secure. Access to all health records should be on a 'need-to' only basis. Some surgeries with a permanent Internet connection may need to investigate the necessity of a firewall to protect their system from 'hacking'. Contact your local Divisions' IM/IT Officer for assistance.
- It is essential that GPs that utilise electronic transfer of health information employ adequate encryption software. If you have not applied for PKI then do so immediately. Contact HeSA on **1300 660 035** or your local Division for more information.
- Health providers must take steps to destroy or permanently de-identify any personal information that is no longer used or being disclosed. GPs may consider permanent secure archiving in preference to destruction of patient health records.

NPP 5 - Openness

An organisation must have a policy document outlining its information handling practices and make this available to anyone who requests it.

- It is advisable that all GP surgeries have a section in their Policy and Procedures document that specifically relates to this Principle as well as the other NPPs. Such a section may be called a 'privacy policy'. The following is a list of things that should be included in a 'privacy policy':
 - the kind of personal information an organisation holds;
 - the main purpose for which the organisation uses that information;
 - how information is disposed of when it is no longer being used;
 - the steps an individual needs to take if they think the organisation may hold personal information about them and they wish to get access to it;
 - whether the organisation is bound by the NPPs or a separate code approved under the Privacy Act;
 - any exemptions under the Privacy Act that might apply;
 - how an individual can complain about possible breaches of privacy;
 - any other relevant matters, such as activities that are outsourced or subcontracted; and
 - contact details of the organisation.
- GPs are also advised to actively promote their privacy policy. This could be simply a matter of having a sign on a wall or notice on a website stating that "This organisation adheres to the National Privacy Principles. A copy of our Privacy Policy is available on request". If someone enquires for more information they can then be provided with a full transcript of the organisations 'privacy policy'.

NPP 6 - Access & Correction

An organisation must give an individual access to the personal information it holds about that individual on request. Access can be denied if providing access would pose a serious and imminent threat to the life or health of any individual or to the privacy of any other individual or if the request is frivolous or vexatious or involves information that relates to existing or anticipated legal proceedings. If the individual's identity has been verified then access should be provided within 30 days of request. Personal information that is inaccurate should be made accurate, complete and up-to-date.

- The NPPs do not allow a fee to be levied against an individual accessing their personal information, however, they do allow for charges associated with the provision of copies of personal information. Any charges levied should be justifiable. They should not be excessive or prevent or limit access.
- Individuals should be provided an opportunity to discuss their personal information when they receive it.

- If a consultation is solely for providing access to health records no Medicare rebate applies, however, a non-rebatable fee may be raised. The individual should be informed of any consultation fees payable when they make their appointment.
- An individual can ask for health information to be updated or modified if he or she thinks it is not current or inaccurate. Difficulties may arise if an individual challenges a GPs opinion, evaluation, diagnosis or decision and seeks to have this corrected.
- In correcting information contained in the health record, GPs are advised not to erase information or opinion but to simply attach to the record an amendment. Individuals also have the right to add their own statements to the health record if they so choose (without modifying the original record).
- Individuals must be able to access any personal information held about them, regardless of whether that information is held by the organisation that collected it or by a (sub) contracting organisation.

NPP 7 - Identifiers

An organisation must not adopt, use or disclose an identifier that has been assigned by a Commonwealth government 'agency' (eg: Medicare number or Veteran's Affairs number) unless use or disclosure is necessary to fulfil its obligations to the agency.

- A Commonwealth agency identifier can only be used for its prescribed purpose.
- An individual's name or ABN is not an identifier.

NPP 8 - Anonymity

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do so. The option of anonymity cannot be denied simply because it is inconvenient.

NPP 9 - Transborder Data Flows

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

NPP 10 - Sensitive Information

An organisation must not collect sensitive information unless the individual has consented, it is required by law, or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety, or where it is impractical to seek consent. In such cases, information should be permanently de-identified before it can be disclosed.

- In special circumstances, any sensitive information collected should be done so in accordance with professional rules of confidentiality. If personal information is not collected for reasons of providing a health service to that individual but for reasons of public health or safety (eg: research) then an organisation must take steps to permanently de-identify the information before it is disclosed.
- Sensitive information is: information or an opinion about an individual's racial or ethnic origin, political opinions or affiliations; religious beliefs or affiliations or philosophical beliefs, memberships of trade associations or unions, sexual preferences or practices or criminal record, that is also personal information or health information.

Disclaimer

This guide has been developed for the benefit of general practitioners by the Alliance of New South Wales Divisions after reviewing the Privacy Act 1988, the Privacy Amendment (Private Sector) Act 2000, the National Privacy Principles (NPPs) and the Guidelines on Privacy in the Private Health Sector, issued October 2001. This guide is not intended to represent a legal discussion of either Act nor should it be substituted for legal opinion. For more information on the National Privacy Principles, or the Privacy Act, contact your local Division or the Alliance of NSW Divisions on 92392900.
