Explaining the National Privacy Principles

The National Privacy Principles (NPP's) set the minimum standards for privacy that the non-government sector has to follow are embodied in the Act and summarised below.

NPP 1—Collection

This principle sets out what a person has to be told when information is collected about them. As applied to a doctor, counsellor or any provider of a health service, NPP 1 requires that:

- only information necessary to deliver the health service be collected
- collection must be fair, lawful and not unreasonably intrusive

The person about whom personal information collected is told:

- the name and contact details of the organisation collecting their information,
- why their health information is being collected,
- how it will be used,
- to whom it may be given,
- that they can access information held about them if they wish
- ilf there is any law requiring collection of the information.
- a person must be told about the main consequences, if any, if the person does not provide all of the information requested.
- the information is collected primarily from the person, but where it is collected from other sources eg. X-rays or specialists' reports, the person should be told this.

NPP 2—Use & Disclosure

This principle sets out how health information once collected can be used (in service) and disclosed (to others outside the practice or service, say members of a treating team), and the consent requirements for such use and disclosure. A
Health organisation should only use or disclose information:

- for the 'primary purpose' (and there is to be only one such purpose) for which it was collected; or
- for directly related secondary purposes which are within the person's reasonable expectations; or
- for use and disclosure for which the person has given consent;
- where other provisions under NPP 2 relating to the public interest, such as law enforcement and public or individual health and safety, apply, such as, for example where it is reasonably believed that the use or disclosure is necessary to lessen or prevent "a serious and imminent threat to an individual's life, health or safety" or "a serious threat to public health or public safety". Health Professionals should familiarise themselves with the terms of the exceptions under NPP 2.
- In other words, once a person has given personal information, the health practitioner must get the client's further consent to use or disclose it. Exceptions to this include use or disclosure of the information for the main reason for which it was originally collected or for other directly related purposes if it would be reasonable for the client to expect this.
    - This is perhaps the main concern for health professionals who need to share client information with treating teams, some of whom don't see the client at the time of collection to get consent or discuss purposes of disclosure. Client understanding of the purpose of collection is therefore crucial. If the main purpose is for treatment, disclosure, for example, for medical research, is a secondary use. Obtaining informed consent to collect information for a holistic approach to client care - that is, care not restricted to the immediate circumstances, but for the client's general health - can obviate the need to obtain consents for handling the same information on subsequent occasions. It is therefore important for efficient clinical practice that doctors clearly identify the primary purpose of collecting information and align their expectations with those of the client.

Note: Taking of family histories without family members' consent

As information is often collected from clients about others in the course of taking a family or social history, good clinical practice would be hindered if NPP 1 and NPP 10 had to be strictly complied with. In recognition of this the Federal Privacy Commissioner first issued a Temporary Public Interest Determination (TPID) and subsequently issued an ongoing Determination (PID) that relieves health service providers from the obligation of obtaining the other person's consent, and explaining to them how the information about them will be handled when taking histories from a client.

NPP 3—Data Quality

This principle sets standards for keeping health information accurate, complete and up-to-date. Good clinical practice requires this. Counsellors and staff are now obliged to take reasonable steps to ensure this is done.

NPP 4—Data Security

This principle sets standards for protecting and securing health information from loss, misuse and unauthorised access. Again, health service providers must take reasonable steps to achieve this. Paper and electronic records must be properly secured, safely stored and maintained. This includes safe disposal of data no longer in use. Electronic data on computer hard disk drives are often retrievable unless correct procedures are used to "wipe" the drives completely clean. Safe disposal of all kinds of computers must take this into account. The cleaning is not difficult but in cases of uncertainty, the services of an IT professional may be appropriate. The safe daily disposal of waste paper bins must take into account identifiable health information on paper scraps. Services are probably doing this responsibly, but the development of e-health records reinforces the need to review and upgrade security measures.

NPP 5—Openness

Health service providers must develop a policy document that clearly explains how the organisation handles health information and make the policy available to anyone who asks. This is a new compliance obligation.

NPP 6—Access & Correction

Generally speaking, individuals have the right to access their own health records and to have information corrected if it is inaccurate, incomplete or out of date. This right includes access to factual and opinion material, including specialists'
reports whether or not a report states that it is not to be shown to the client without the specialist's consent. This is a new legal requirement effecting a change in practice, and requires new understanding and procedures.
Access can be restricted or denied in certain circumstances specified in the Act, for example, where access might pose a threat to a person's life or cause serious harm to a person's health.

NPP 7—Identifiers

Generally speaking, an organisation must not adopt as their own identifier, Commonwealth government identifiers, such as a Medicare or Veterans Affairs number, and must not use or disclose such identifiers except to fulfil its obligations to the agency which assigned the identifier.

NPP 8—Anonymity

Where lawful, and practicable, individuals must be given the option to interact anonymously. In the context of health care this is likely to apply in only in some special circumstances, for example where treatment or counselling is
provided on an anonymous basis in the area of HIV/AIDS and sexual health. Providing a safe health service, and for billing and rebate purposes, services are required to record the identity of the client.

NPP 9—Trans-border Data Flows

An organisation can transfer personal information out of Australia only to countries bound by similar privacy protection laws or schemes, unless the individual otherwise consents. This principle is to ensure continued privacy of client information beyond Australian jurisdiction.

NPP 10—Sensitive Information

An organisation must not collect sensitive information without the individual's consent, unless the collection is required by law, or falls within some specified limited circumstances. Health information is 'sensitive information'.
Exceptions include: – where collection is necessary to prevent a serious and imminent threat to the life or health of an individual and the individual is physically or legally incapable of giving consent or is physically unable to communicate consent;

- where collection is necessary for the establishment, exercise or defence of a legal or equitable claim (this may include many medical defence purposes);

- where the information is necessary to provide a health service to that individual and is collected as required by law or in accordance with binding rules established by competent health or medical bodies that deal with professional confidentiality;
- where the information is collected for research relevant to public health or public safety, in cases where:
- the purpose cannot be served by de-identification,
- obtaining consent is impracticable, and
- the information is collected in accordance with the law or approved rules of certain bodies or guidelines approved by the Commissioner under section 95A of the Act for this purpose.
-

It is important here to note that: **Sensitive information** means information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, or criminal record, as well as health information about the person.

Health information includes personal information collected to provide, or in providing, a health service. **Personal information** means information or an opinion, including information or an opinion forming part of a database, "whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion". This means that consent of the individual is required before any personal, sensitive or health information is collected in the course of providing a health service.

Are the NPP's retrospective?

NPP 6 relating to an individual's access to information applies to information collected on or after 21 December 2001, and also to information collected before 21 December which is referred to, used or disclosed after that date. If compliance in giving access to information collected prior to 21 December poses an unreasonable administrative burden or expense, then access need not be granted; however, provision of a summary would be an option to consider.
NPP 4 on data security, NPP 5 on openness, NPP 7 on identifiers and NPP 9 on trans-border data flows also apply to information collected before 21 December 2001. Otherwise the rest of the NPP's apply to information collected after 21
December 2001.