Policy

Directive: compliance is mandatory

Code of Fair Information Practice

Objective file number: 2010-00843/1
Policy developed by: Policy and Intergovernmental Relations
Approved at Portfolio Executive on: December 2001
Next review due: 30 June 2012

Summary The Code of Fair Information Practice outlines the circumstances under which personal information can be collected, used, stored and disclosed

Keywords Privacy, information, confidential information, personal information, records, data, directive

Policy history
Is this a new policy? **N**
Does this policy amend or update an existing policy? **Y**
Does this policy replace an existing policy? **Y**
If so, which policies?

Applies to All SA Health Portfolio

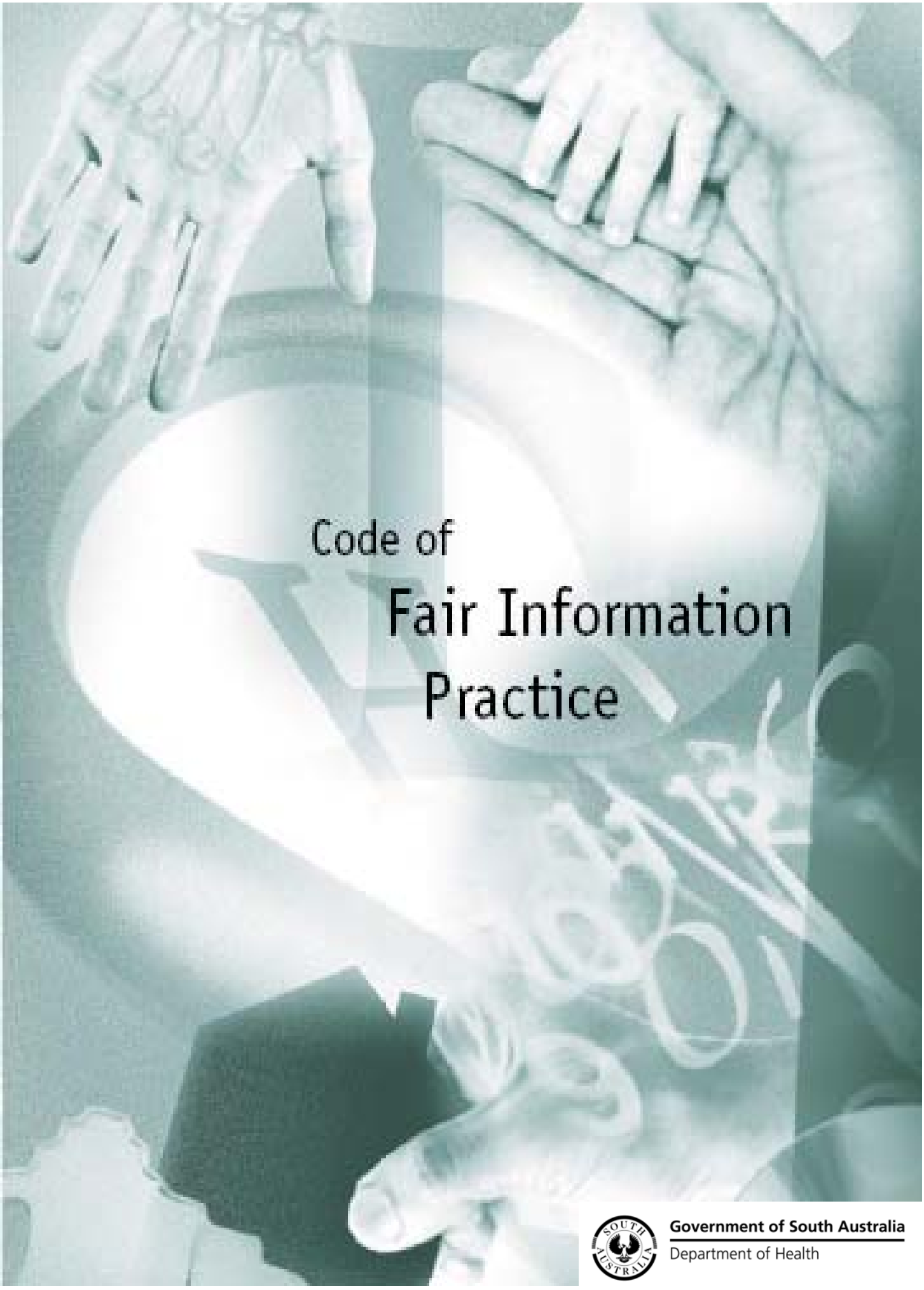
Staff impact All Staff

PDS reference D0067

Version control and change history

Version	Date from	Date to	Amendment
1.0	02/2002	06/2004	Original version
2.0	06/2004	07/2006	
3.0	07/2006	current	Changed to reflect split of DHS

Government of South Australia
SA Health



Code of Fair Information Practice

Government of South Australia
Department of Health

CONTENTS

FOREWORD

The role of the Department of Health is to provide access to services that enhance and protect the health, social wellbeing and quality of life for the community. The Department's vision encompasses the provision of more coordinated responses to the health needs of the community. To realise this vision, each of the Department's corporate strategies is dependent upon appropriate information management and communication services.

The Department of Health is responding to the opportunities that information technologies offer with respect to the delivery of a wide range of health services to the community. The substantial benefits arising from the increased use of new information technology include improved delivery of client services, enhanced public health protection and more effective planning and research activities.

Information is regularly collected by the Department, its funded service providers, contractors, consultants, volunteers, etc., to assist with the provision of services to clients. This information is subsequently used to further enhance the quality of service provision through more informed and client-centric decision-making at the corporate and service delivery levels of the Department and funded service providers. Furthermore, information may be used for research into the impact of current service delivery, thereby providing a basis for recommending service improvements.

Providing services in the area of health inevitably involves handling large quantities of personal information that is often highly sensitive. Consequently, there is growing community concern regarding privacy when providing personal information to any organisation. The willingness of consumers to accept new technologies is closely tied to their confidence in Government agencies and other organisations to handle their personal information in a fair, secure and appropriate manner. Consequently, it is critical that we ensure that any concerns from individuals about protecting the privacy of their personal information are appropriately addressed. The South Australian State Government views the protection of privacy as a crucial foundation for electronic product and service delivery on a day-to-day basis, as well as for longer term strategic planning and research initiatives.

The Department of Health has developed a Code of Fair Information Practice to outline what it and its service providers should do, and what clients can expect, in protecting personal information. This is balanced against the genuine, controlled and legitimate use of personal information in providing and improving service delivery to clients. This Code provides a framework to ensure that personal information privacy issues are handled in an appropriate manner across the Department and its funded service providers. In developing its own Code, this Department is endeavouring to provide both initiative and leadership in this important area of community and public concern.

The Principles set out in this Code provide guidance on all aspects of handling personal information for both staff of the Department, funded service providers and others who have access to Departmental personal information. The Explanatory Notes, which will be updated from time to time as required, provide a more in-depth explanation of how the Principles should be applied.

The standards set in this Code are based on the National Privacy Principles (NPPs) contained in the Commonwealth *Privacy (Private Sector) Amendment Act 2000* which are applicable nationally to the private sector. These Principles are based upon existing national and international privacy regimes, thereby enabling the Department to meet external Government, business and community expectations.

The Department of Health would like to acknowledge the work undertaken by the Commonwealth Privacy Commissioner and his staff in the development of the NPPs and the NPP Guidelines upon which the Code is largely based.

INTRODUCTION

WHAT IS A CODE OF FAIR INFORMATION PRACTICE?

Fair information practices aim to ensure that organisations which hold information about individual people handle that information responsibly. This generally means that, wherever possible, people should be able to exercise some control over the way information about them is collected, used, stored and disclosed.

While confidentiality is an essential element of the relationships between individuals and the providers of health, housing and community services, the individual's right to privacy for their personal information is relative and not absolute. In addition to serving the interest of the individual, personal information may also be used to service legitimate needs of other individuals and organisations. Initiatives to improve individual and community health, housing and welfare depend upon the accumulation of, and access to, personal information. Thus, the requirements of the community for information privacy protection need to be considered and balanced with justified claims from other interested parties.

This Code of Fair Information Practice provides part of an information management framework that will apply across the Department and its funded service providers and to others with access to Departmental personal information. It outlines what is expected of service providers and their clients in order to establish and maintain a structured environment for the management of personal information, whereby the privacy of the information is protected without hindering its use for other legitimate and justified purposes.

NEED FOR A CODE OF FAIR INFORMATION PRACTICE

The Department needs to be able to derive maximum benefit from emerging information and communication technologies in leveraging improved information access and management. Communication and information technology infrastructure is required to support business efficiency and effectiveness leading to improved public health protection and service delivery, providing more informed decision-making for strategic planning and operational management, and supporting research and the development of new business strategies.

The nature of the health, community services and housing programs, along with the types of personal information collected, present specific demands upon the Department's information management requirements. For example, the transition towards some new systems requires the development of integrated databases of personal information. Access to this integrated data has led to the development of new and improved ways to deliver effective care, identify and treat those at risk from disease, conduct population-based research, and assess and improve service delivery. However, these uses of personal information may raise understandable concerns about protecting the privacy of this information. Thus, while endeavouring to exploit the benefits of integrated enterprise-wide electronic information management systems, the Department needs to be cognisant of concerns regarding the privacy of personal information.

The Department has shown its commitment to the privacy of personal information by developing an information privacy protection framework to apply across the Department and its funded service providers. The benefits of this framework include:

- providing **coherency** across the Department in relation to how privacy issues are addressed through consideration of information privacy protection principles;

- building **client confidence** in the ability of the Department to protect and manage their information in accordance with acceptable privacy principles that are consistent with national and international standards;

- allowing the Department to have **privacy-sensitive information handling practices** which accords with the current requirements for South Australian Government agencies and aligns with legislative developments in other Australian jurisdictions; and

- supporting the **necessary balance** between the protection of personal privacy and the professional conduct of activities to assure and improve public health protection, quality of services, evaluation and research, which are all-important aspects of the provision of services.

To successfully fulfil these outcomes, this Code of Fair Information Practice will be supported by a suite of complementary "tools", which collectively, create a "structured information management framework". These "tools" include:

- A **Communications Strategy** to raise awareness and promote adoption of the privacy principles outlined in this Code;

- **Education and training programs** to ensure that users have the requisite knowledge and skills to implement the Code and comply with its information privacy principles;

- A **Privacy Impact Assessment** methodology for evaluating the privacy impacts of new proposals that involve personal information;

- A **Privacy Compliance Audit** to assess compliance with the privacy principles outlined in this Code;

- **Complaint Handling Mechanisms** to deal with claims from individuals that the Department or funded service provider has committed an act that breaches their privacy; and

- Responses to **Frequently Asked Questions** and **Information Sheets** to assist with further clarification and interpretation of the Code.

Information regarding these support materials will be available as separate publications.

WHAT IS INFORMATION PRIVACY?

While there have been many attempts in the past, there is yet to be a definitive definition of privacy. In the 1890s, future US Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone". Alan Westin, an author, in 1967 defined privacy as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others".

Information privacy refers to:

> *a group of related rights (legal and ethical) regarding an individual's control over the collection, use, storage and disclosure of their personal information*

"Personal information" is defined (in this Code) to mean:

> *information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion*

"Whether recorded in material form or not" means that the information can appear in any form (e.g. sound, image, text or biologically based) and be recorded in any medium (e.g. print or electronic).

For the purpose of this Code, it is useful to distinguish between ***privacy***, ***confidentiality*** and ***security***:

Information Privacy refers to:

> *the rights of an individual to exercise some control over the way information about them is collected, the way in which it may be used, who it may be disclosed to, and ensuring that the information is securely stored and not misused. It also refers to the right of an individual to have access to information concerning him/herself and to ensure that, when information is used or disclosed, it is not incorrect, out-of-date or misleading.*

Confidentiality refers to:

> *the responsibility of custodians and recipients of personal information to ensure that it is not disseminated to unauthorised users.*

Security refers to:

> *a set of procedures, techniques and technologies employed to protect information from malicious or accidental destruction, alteration or access.*

NEED FOR INFORMATION PRIVACY

There are substantial benefits to be gained through the computerisation of individual records. It can lead to: improved public health; reduced service delivery costs; increased access to services; and improved quality of service delivery. Information contained in electronic form can be more efficiently collected, stored, analysed and transmitted. As such, it can be accessed more easily for direct client care, to coordinate care, and in emergency situations. It also can be analysed more readily to reveal population-based trends and serve to reduce administrative costs by more easily transmitting information. Hence, advancements in information technology and telecommunications, including the Internet,

have emerged as key tools for delivering improved efficiencies and effectiveness in the delivery of health, housing and community services.

However, there is growing concern regarding the protection of personal privacy and it is likely that the growth of electronic based information management systems will exacerbate this problem. The magnitude of the threat to personal privacy increases significantly when records are computerised. These developments raise the following concerns in relation to personal information privacy protection.

- Increasing the capacity to handle (collect, store, sort and distribute) more information may weaken previous barriers inherent in collecting and storing only the personal information that was essential;

- Increasing the potential to integrate information from different sources to support more-informed decision-making may increase the likelihood of using information for unjustified purposes;

- The growing demand for an increased capacity to link information brings with it pressure for a higher integrity of such information. The sensitivity of some types of information demand that robust controls on the use and dissemination of any such information will be necessary;

- Increases in the number of organisations collecting and storing personal information, that are not bound by professional codes of ethics or common-law duties of confidentiality, means they often have fewer obligations, and little guidance, on how to protect this information;

- Uses of personal information that extend beyond the individual's current knowledge and expectations, especially when inconsistent with the original purpose for which the information was gathered, can undermine the individual's trust and willingness to share information with their health, housing and/or community service providers; and

- If information is incomplete or inaccurate, it will be less reliable for broader service improvement initiatives. Ultimately, the public's concern over the loss of privacy could become so great as to undermine the quality of their health, housing, welfare and community services.

In order to realise the benefits derived from electronic records, there needs to be a balance between protecting the privacy of individuals and society's requirements for information to benefit all individuals.

Strong privacy protection can help to build client trust and ensure that when information is shared, it is complete and reliable. Furthermore, while new information technologies offer additional benefits for privacy protection through improved security, limiting access, monitoring users and stripping data of individual identifiers before it is shared with third parties, they do not resolve the larger policy questions about how data should be used shared and exchanged. The technology can help to protect information, but only privacy policies and principles can articulate what limits are appropriate.

BALANCE BETWEEN PRIVACY PROTECTION AND OTHER INTERESTS

To benefit from advancements in information technologies, the requirements of the community for privacy and confidentiality need to be balanced by society's requirement for increased access to information. The Australian Law Reform Commission has described this balance as follows:

> *None (of the attempts to define privacy) is completely satisfactory. In part, this is because privacy is a collection of related interests and expectations, rather than a single coherent concept. Claims to privacy must be seen in the appropriate context, as an expression of the claim that all human rights be appropriately respected.*
>
> *Any claim by an individual to preserve his own integrity by ensuring respect for his privacy must be considered against similar, equally justified claims by other individuals. It must also be considered against the need to help society at large in its efforts to improve the lot of individuals within it by ensuring the efficient running of government, industry, commerce, professional activity and research. None can be completely ignored. Privacy is but one of a number of human rights. Privacy protection should not ignore other legitimate interests.*

If the limits placed on use and disclosure of personal information for purposes other than its primary reason for collection are so strict, then any of the benefits that may result from its use and disclosure for secondary purposes will be more limited than if it had been made freely available for these purposes.

Conversely, if the level of protection were low, people would become concerned about losing control over their personal information and subsequently become reluctant to take up the opportunities offered by the new technologies. Furthermore, they may develop 'privacy protective' behaviours, such as withholding information, lying or avoiding care or visiting different practitioners to avoid having all their information held by one organisation.

The individual's rights to privacy for their personal information are not absolute. Hence, privacy protection is a 'balancing process'. The rights of individuals need to be balanced against other public interests and with competing claims from other individuals, businesses and organisations. However, the approach, if not carefully managed, may not serve the best interests of either the individual or service providers. The preferred solution is to integrate privacy protection principles into general information practices.

This Code aims to address this balance.

WHAT TYPE OF INFORMATION IS COVERED UNDER THE CODE?

The Principles contained in this Code relate to "**personal information**".

Personal information is defined as:

> *information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion*

This includes information from which the names and addresses have been removed, but where sufficient information remains that the identity of the individual could potentially be identified (for example, by way of a number or reference which, when combined with other information, can be related to an individual/subject).

The Principles apply to personal information **regardless of it's format**. For example: it includes paper or electronic records, videos, x-rays, photographs, specimens, entries on computer databases, and genetic information.

The Principles do not apply to **de-identified information**, where all personal identifiers have been removed or altered such that there is no possibility of identifying, or linking it back to, the subject's identity.

Nor do the Principles apply to **employee records**.

WHAT PRIVACY PROTECTION PRINCIPLES APPLY TO THIS CODE?

The Principles contained in this Code are based upon the national privacy principles which form the key provisions of the Federal Government's *Privacy (Private Sector) Amendment Act 2000.*

These principles provide an ideal basis for this Code because they are generally applicable to the private sector[1], particularly those organisations which collect, use, store or disclose "sensitive information" - much of the type of data held by the Department of Health and its service providers.

In adopting the National Privacy Principles, the Department of Health is aligning as much as possible to what looks likely to be the model for a nationally consistent scheme for managing personal information.

The National Privacy Principles (NPPs) differ somewhat from the Information Privacy Principles (IPPs) which are the basis for the 1989 Cabinet Administrative Instruction on privacy. This Instruction applies to all State Government agencies, including the Department of Health. Where the two sets of principles differ, the Privacy Committee of South Australia (which oversees the scheme established by the Cabinet Administrative Instruction) has granted limited exemptions to enable the Department to adopt the NPPs.

[1] The Privacy (Private Sector) Amendment Act 2000 requires "organisations" in Australia to abide by the National Privacy Principles contained in that Act. Most State and Territory Government bodies, such as departments, are not bound by this Act. See the Commonwealth Privacy Commissioner's Information Sheet No. 6 for more information.

WHO NEEDS TO APPLY THE PRINCIPLES IN THIS CODE?

This Code is intended to apply to all employees who, in the course of their work (whether paid or voluntary), have access to personal information collected, used or stored by or on behalf of the Department of Health and/or funded service providers. This includes:

- **All staff of the Department of Health**, whether paid or not, whenever they handle personal information, whether it relates to clients or any other individuals. They will also need to consider these Privacy Principles during the development of new initiatives or proposals that may involve the management or handling of personal information. All personnel with access to personal information should undertake to abide by privacy principles that reflect the requirements of this Code. Their undertaking to abide by these principles should remain in effect even after they cease to be employed by the Department or funded service provider. This requirement should be included in job descriptions and performance agreements.

- **All staff of funded service providers** (including hospitals and non-government organisations*), as well as any individual or organisation to whom they sub-contract work. This requirement should be clearly spelt out in service agreements with funded organisations and should clearly set out responsibility for data security in transit, restrict the uses to which the information can be put, permit only authorised disclosures and include requirements for secure storage.

- All **consultants*, contractors*** (including information technology (IT) contractors who process data on behalf of the Department) and **sub-contractors*** are required to adhere to the standards in these Principles. Contracted staff, or a responsible representative of every company contracted for data entry or other work which necessitates accessing personal information, should sign a confidentiality agreement and be given a copy of this Code. The agreement should clearly set out responsibility for data security in transit, restrict the uses to which the information can be put, permit only authorised disclosures and include requirements for secure storage. This requirement should be included in all contracts issued by the Department, including those where the Department is **outsourcing** a function.

- Any **private agencies*** or **practitioners***, **researchers*** or others (including volunteers and students) who have access to personal information collected by or for the Department of Health and funded service providers will be required to acknowledge/observe this Code. This requirement should be subject to signed undertakings or agreements.

*If the information relates to personal **health information** then the private sector organisation to which the information is provided may be subject to the NPPs contained in Commonwealth *Privacy (Private Sector) Amendment Act 2000* or a Code approved under that Act. If this is the case, the organisation will need to acknowledge it's obligations under that Act.

WHO IS RESPONSIBLE FOR ENSURING ADHERENCE TO THE PRINCIPLES CONTAINED WITHIN THIS CODE?

To implement privacy protection procedures successfully, staff need to be aware of the underlying principles of information privacy as well as their responsibilities in complying with this Code.

This Code therefore places certain obligations on the Department, or staff within it, for:

- **Raising awareness**
  Senior management within agencies and other service providers that, in the course of their work, have access to personal information are responsible for ensuring that their staff are familiar with the privacy principles within this Code. This will generally involve providing staff with appropriate awareness and training (a **Communication Program**).

- **Training**
  Staff that have access to personal information should receive appropriate training to enhance their understanding of the privacy protection principles and to assist them to execute their responsibilities under the Code. Senior management within agencies and other service providers are responsible for ensuring that training is made available to all relevant staff, including new employees, volunteers, students, temporary and contract staff (an **Education and Training Program**).

- **Compliance audits**
  The onus is on the individual staff member to ensure that the Privacy Principles are adhered to. It is their responsibility to demonstrate, for the purposes of audits and complaints investigations, that personal information has been handled in accordance with the relevant Principles. However, information is usually handled within a supervisory context, in which case, the supervisor has a corresponding responsibility to ensure information about these Principles is readily available to staff and that training has been conducted where necessary.

Each agency should designate an officer to whom all request for guidance on this Code should be referred and who is responsible for ensuring that all principles are observed. This officer should also be responsible for conducting self-assessment and audits of the agency's information handling practices.

HOW DO THESE PRINCIPLES RELATE TO OTHER POLICIES?

This Code supersedes previous policies dealing with the collection, use, storage and disclosure of personal information developed in parts of the Department. However, in the process of implementing this Code, it may be useful to review and reintroduce some of these policies under the auspices of the Code.

Where an exemption from any aspect of the Code is sought, the matter will be considered initially by the Research Policy and Ethics Unit. Where granting the exemption would entail an exemption from one or more of the Principles contained in the Code, it is likely that an exemption from Cabinet Administrative Instruction 1/89 “The Information Privacy Principles” will also be required. Where this occurs, the request will be forwarded to the Privacy Committee of South Australia. This Committee, established by proclamation in 1989, has the authority to grant such exemptions.

Departmental and Divisional Research, Ethics and/or Privacy Committees are responsible for approving the use of personal information for research purposes. In general, these Committee utilise/observe the guidelines of the National Health and Medical Research Council (NHMRC). Guidelines, issued under Section 95A of the Privacy Act 1988, provide a framework in which medical research involving personal information should be conducted to ensure that such information is protected against unauthorised collection or disclosure (www.health.gov.au/nhmrc/publicat/order.htm).

SUMMARY OF THE PRINCIPLES

The table below provides broad summary information relating to the general provisions and intent of the Principles contained in this Code. The phrases in bold and italic give an indication of what the Principles mean to clients/individuals.

Principle	Relates to:	Intent
COLLECTION		
1.1	**Purpose** of collecting personal information	***We will only collect information that is necessary for what we do.*** Limit information we collect to only that which is necessary for one or more of our legitimate functions or activities. The onus is on the collector to justify why certain personal information is being collected (see Principle 1.3).
1.2	**Manner** of information collection	***We will be fair in the way we collect information about you***. Personal information will be collected by lawful, fair and non-intrusive means to prevent undue pressure or coercion being placed on individuals when information is collected.
1.3	**Notification** regarding data collection	***We will tell you who we are and what we intend to do with information about you*.** At or before personal information is collected, reasonable steps will be taken to inform clients why their personal information is being collected, the use to which the information will be put and their rights to access this information. (See also Principle 1.5)
1.4	**Source** of personal information	***Where practicable, we will collect personal information directly from you.*** Where reasonable and practicable, personal information will be collected directly from the individual to whom the information relates.
1.5	**Notification** regarding data collection from third parties.	***If we collect information about you from someone else we will, wherever possible, make sure you know we have done this.*** If the personal information is collected from a third party, wherever possible, individuals will be similarly informed of all matters dealt with item 1.3 above.

USE AND DISCLOSURE		
2	**Use** and **disclosure** of personal information.	***We will only use or disclose information about you in ways that are consistent with your expectations or are required in the public interest.*** Use or disclosure of personal information will normally relate to the primary purpose of collection.
DATA QUALITY		
3	**Accuracy** of personal information	***We will ensure that information about you is accurate when we collect or use it.*** When personal information is collected, used or disclosed, reasonable steps will be taken to ensure it is accurate, complete, up-to-date and not misleading.
DATA SECURITY		
4	**Security** of personal information held	***We will keep information about you secure.*** The personal information held within the Department of Health and funded service providers will be protected from misuse and/or loss from unauthorised access, modification or inappropriate disclosure by unauthorised individuals and/or organisations. Where authorised under the State Records Act, personal information should be destroyed or permanently de-identified in a secure manner when no longer required.
OPENNESS		
5	Maintaining a **policy of openness**	***We will be open with you about what kinds of personal information we hold and what we do with it.*** A policy of openness, transparency and accountability will be adopted for the management of personal information. Clearly expressed policies will be developed to ensure that individuals are kept informed about what kinds of personal information are held, for what purposes, how it is held, how it will be used and if it will be transferred or disclosed to a third party.
ACCESS AND CORRECTION		
6	Right to **access** and **correct** personal Information	***Wherever possible, we will let you see the information we hold about you and correct it if it is wrong.*** When we hold personal information about an individual, wherever possible (in accordance with the Freedom of Information Act), it will provide the individual with ready access to it. Reasonable steps will also be taken to correct personal information if it is found to be inaccurate, incomplete, misleading or not up-to-date (in accordance with other legislative provisions - including the Freedom of Information Act, Evidence Act and State Records Act).

UNIQUE IDENTIFIERS		
7	Unique **identifiers**	***We will limit our use of identifiers that government agencies have assigned to you*.** Assigning and using unique identifiers by government agencies should be limited and used in an appropriate manner.
ANONYMITY		
8	**Anonymity** for individuals	***If we can (and you want to) we will deal with you anonymously*.** Wherever it is lawful and practicable, individuals will have the option of not identifying themselves when their personal information is collected.
TRANSBORDER DATA FLOWS		
9	Security of personal **information during transmission**	***We will take steps to protect your privacy if we send personal information about you to a third party.*** Reasonable steps will be taken to maintain the security and protect the privacy of personal information if it is transferred on to a third party.
SENSITIVE INFORMATION		
10	**Sensitive** personal information	***We will limit the collection of sensitive information about you.*** Wherever possible, the collection of personal information, such as that revealing political opinions, religious or philosophical beliefs, trade-union membership, or details on health or sex, will be limited (except under specific circumstances).

THE PRINCIPLES

The following sections provide guidance on the application and interpretation of the Principles which form the basis of this Code.

Each Principle forms its own section and contains:

- the Principle;
- the issue(s) addressed by the Principle;
- the intended outcome of the particular Principle;
- guidance on how the Principle is to be applied, including definitions and interpretation; and
- particulars regarding possible exceptions (ie the circumstances under which it may not be possible to comply with a Principle).

A full set of the Principles is attached as Appendix B.

PRINCIPLE 1: COLLECTION

1.1
The Department of Health and funded service providers must not collect personal information unless the information is necessary for one or more of its functions or activities

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Purpose for collecting personal information.

Intended privacy protection outcome(s)

The aim of this Principle is to enable people to exercise some control over the handling of their personal information by limiting its collection to only that which is **necessary.**

Application of the Principle

When we collect personal information, it should be limited to collecting only the information that is considered **necessary for providing a particular service or fulfilling a particular function.** These services and/or functions may include:

- providing a service to a client;
- billing activities;
- monitoring client care;
- managing Departmental responsibilities; or
- protecting public health, housing and welfare through monitoring and investigations.

Limiting the collection of personal information is dealt with in two places. This section of the Code relates to the general collection of non-sensitive information. Collection of "sensitive information" (including personal health information) is dealt with under Principle 10.

In relation to the general collection of information, the onus is on us to justify why particular details regarding personal information are collected from individuals (see also Principle 1.3 below). This serves to deter the routine collection of “non-essential” information on the grounds that it may be useful in the future, which may lead to significant amounts of “non-essential” information about individuals being held.

Determining what information is "necessary"
Placing limits on collecting only necessary information involves determining, at the outset, exactly what details are needed or, at the very least, developing guidelines on the kind of information which it would be appropriate to collect in certain circumstances. Hence, the privacy protection implications from any new data collection activities should be assessed in advance.

"Necessary" should be interpreted in a practical, not theoretical or in-principle, sense. If a legitimate function or activity cannot be effectively performed without collecting personal information, then that personal information would be regarded as necessary for that particular function or activity.

At the time of collection, it may sometimes be difficult to determine what information will be required in the future. However, this uncertainty is not sufficient reason to justify collection of additional details that have not yet been identified as relevant for a particular purpose. The emphasis should be on identifying what information is relevant for a particular purpose(s) at the outset.

Possible exceptions

Information collected for research purposes
Health information collected for research purposes is dealt with in the 'Explanatory Notes' on Principle 10. Use and disclosure of personal information for research purposes is outlined under Principle 2.

Collection of 'sensitive information'
The collection of 'sensitive information' (including health information) is dealt with under Principle 10.

1.2
The Department of Health or funded service provider must only collect personal information by lawful and fair means and not in an unreasonably intrusive way

EXPLANATORY NOTES

Issue(s) addressed by this Principle

Manner of information collection.

Intended privacy protection outcome(s)

Ensuring that collection of personal information is undertaken in a **lawful**, **fair** and **non-intrusive** method serves to prevent undue pressure or coercion being placed on individuals when personal information is collected from them. It also requires that staff members are sensitive to the particular circumstances in which personal information is collected.

Application of the Principle

This Principle requires us to only collect personal information by lawful and fair means as well as to have regard to the circumstances and environment in which information is collected.

In general:

- **"Lawful"** means we must ensure that measures used to collect information comply with any applicable laws, including:
  (i) Statutes which apply specifically to the Department or a Division's activities; and
  (ii) Any other State or Commonwealth legislation which may be relevant (such as legislation on fair-trading or telecommunications if applicable).

- **"Fair"** means without intimidation or deception.

When collecting personal information, it is important to be sensitive to the individual's particular circumstances. This requires awareness and consideration of any contextual factors and/or influences, such as ethnic and culture background, and the physical surroundings where information collection occurs.

Appropriate responses to ethnic and/or cultural issues may involve:

(i) Providing expanded (i.e. beyond basic requirements of Principle 1.3) explanations for why certain information is required. For example, collecting information regarding the individual's indigenous status is critical to research and planning aimed at improving Aboriginal health; and

(ii) Providing interpreters and/or multi-lingual application forms and brochures.

Appropriate responses to an individual's concerns regarding the physical surroundings for collecting information may involve a range of measures aimed at providing a private, reassuring and non-threatening environment.

Possible exceptions

There will be some circumstances where covert collection of information by surveillance or other means involving a level of deception, would be considered "fair". Examples would include investigations of possible fraud or other unlawful activities.

In some circumstances, we may need to collect information in a manner that could be considered **intrusive** even though the information is being collected by **lawful** means. For example, collecting highly sensitive information relating to a suspected victim of child abuse without the consent of the child or guardian. In this situation, the applicable legislative provisions prescribing this collection would apply.

The overriding intent is to ensure that the intrusive nature of the collection is limited to that which is necessary to gather the relevant information.

1.3:
At or before the time the Department of Health or funded service provider collects personal information from the subject of the information (or, if that is not practicable, as soon as practicable thereafter), it must take reasonable steps to ensure that the subject of the information is aware of:

(a) the identity of the Department or funded service provider and how to contact it;
and
(b) the fact that he or she is able to gain access to the information;
and
(c) the purposes for which the information is collected;
and
(d) to whom (or the types of individuals or organisations to which) it usually discloses information of that kind;
and
(e) any law that requires the particular information to be collected;
and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Notification regarding data collection.

Intended privacy protection outcome(s)

This Principle is intended to ensure that individuals are aware of who is collecting their personal information, what it will be used for, who will have access to it, and their rights of access to this information. This will also assist us to adopt an appropriate level of openness (refer also to Principle 5) in the way that we handle personal information.

Application of the Principle

This Principle requires, where practicable, that individuals are provided with the advice listed in clauses 1.3(a) to (f) of this Principle:

- before or at the time of collection; and
- in a manner that is easily understood.

Information may be collected by a variety of means including verbally over the counter or during a telephone conversation. When **over the counter**, a brief notice could be prominently displayed and supplemented with more detailed written information. Where information is **collected over the telephone**, it may not be practical to address all of the 1.3(a) to (f) issues at the time of actual collection. If so,

people should be informed of them as soon as possible, for example, in any confirmatory documents.

Whether this advice is provided verbally or in writing, it must be in a manner that is easily understood by the individual. It may therefore be necessary to consider our clients and provide information in languages other than English. For consistency, when providing notification advice, regardless of whether it is verbal or written, it should conform to an agreed standard and format that cover all of the content described in clauses 1.3(a) to (f).

Alternatively, written advice could be provided via application forms, formal notification statements or printed information materials. Where information is being collected on a form, a statement on the form could satisfy the obligations under Principle 1.3.

Informing people about the identity of the Department and funded service providers and how to contact it - 1.3(a)

In many cases when information is collected directly from an individual, it will be obvious who is collecting the information. Where the circumstances of collection make any of the matters in 1.3(a) to (f) obvious, a **"reasonable step"** would be to do nothing. For example, in a large majority of cases, the identity of the Department and funded service providers collecting the information is obvious from the circumstances. However, this will not always be so, for example, when transactions occur via the Internet or where information was being collected at the individual's home or at some other location. In these instances steps may need to be taken to advise of who is collecting the information, for example, by providing a business card or pamphlet which clearly identifies the agency and its contact details.

Informing people that they are able to gain access to the information - 1.3(b)

Steps should be taken, when collecting information, to advise the individual that they are able to gain access to the information. This can be undertaken by providing information in easily understood brochures/information sheets or by prominently displaying signs at the point of collection.

Informing people about the purposes of collection - 1.3(c)

Steps need to be taken to advise an individual why particular information is being collected. In most cases, the description of the **purpose** can be kept reasonably general and provided in such a way that it is easily understood. If the collection is made for only one purpose, the purpose could be inferred simply from the title of a form.

At times, further information may be requested from an individual in addition to that required to provide a particular service. In these situations the individual should be told why that additional information is being sought. For example, it could be to improve the quality of care provided, or to assist in planning and/or research activities. Wherever practicable, the individual should be given a genuine choice about whether or not they wish to supply these additional details. (It should be noted that in the case of legal collections, for example those authorised under the Public and Environmental Health Act, no such choice can be offered. The individual should still however be informed that the information is being collected for this purpose.)

Informing people about usual disclosures - 1.3(d)

When collecting personal information, we should take reasonable steps to advise the individual of our usual practices regarding the disclosure of information to third parties.

'Reasonable steps', in this context, would generally mean providing generic descriptions for categories of individuals and/or organisations to which information may be provided (eg 'State government licensing authorities' or 'health insurers'). Disclosures, such as those under a warrant or to intelligence agencies, would not usually need to be mentioned. Where information may be disclosed to other parts of the Department or to others for planning and/or research purposes, the individual should be assured that the information disclosed would usually be in a **de-identified form** unless otherwise authorised by law, or approved by an appropriate ethics committee, or where the individual gives their **consent**.

If, in the future, an individual's information is required by other organisations in order to protect the individual's health, welfare and safety, and the individual was not notified of this at the time of collection, the individual must be told about these additional uses and disclosures as soon as practicable.

We will sometimes have a legal obligation to disclose certain details about an individual to a relevant authority. For example, there are legal obligations imposed on certain professionals in situations involving ***mandatory reporting*****,** such as under the *Children's Protection Act 1993*, where some professionals are legally required to report child abuse when they suspect it is occurring. In cases where information on child abuse comes to the attention of a professional via a direct disclosure from the abuser, the professional should advise him/her that staff have a legal obligation to notify the relevant authorities. The individual does not need to be advised of this where one of the exceptions (listed below) applies. That is, where such advice would prejudice the health, welfare or safety of the individual, another individual or the community, or where the advice would prevent the Department from carrying out its obligations under the law.

Informing people about any law that requires or authorises the information to be collected - 1.3(e)

This Principle requires that, wherever possible, an individual should be informed about:

(i) any legal obligation or legal authorisation that requires the person to **provide** the information;

or

(ii) any legal obligation or authorisation on the Department or funded service provider to **collect** that person's personal information.

In describing legal obligations you should specify the legislation that imposes the obligation or authorises the collection. This means that staff must be adequately familiar with all relevant legislation.

In addition to information which the individual is legally bound to provide, it is likely that other information may be required to fulfil a function. If an individual queries why certain details are being collected, the reason for the collection should be clearly explained in accordance with Principle 1.3(c), as should the consequences of not supplying the information in accordance with Principle 1.3(e).

Informing people about the consequences of not providing personal information - 1.3(f)

We would not be required to describe every possible consequence of not providing information. This is only intended to apply to significant (and non-obvious) consequences, such as preventing the delivery of certain services. Generally, we should inform individuals of what items of information are essential to fulfil the primary purpose of collection and the consequences of not providing that essential information.

Possible exceptions

Where an individual has regular dealings with us, they may not need to be advised of points 1.3(a) to (f) on each occasion. However, unless the person collecting the information is reasonably sure that the individual has been made aware of them (for example, because the client is attending a related follow-up consultation with the same professional), then the individual should be notified of these points whenever new or additional information is collected from them.

The main point is that the individual needs to be made aware of these matters; the Principles would not require an individual to be repeatedly and specifically told the same thing every time they have contact with us.

There will be instances where it is not "reasonable or practicable" to provide an individual with details about the collection of information. This would include instances where notifying at the time of collection would **defeat the entire purpose** of a legitimate activity of collection. For example, this exception would apply where information was being collected for the purpose of investigating fraud or some other illegal activity.

Another exception to advising individuals about the collection of their information is applicable in the health sector when collecting medical history information. Health professionals routinely seek information about an individual's family, social or medical history and this often results in the collection of information about someone other than the individual concerned. For example, seeking information about a family history of breast cancer, may result in the collection of information about the individual's mother, sister or auntie. In this circumstance, it is not necessary to advise the mother/sister/auntie that their information has been collected, provided:

- the collection of the third party's information is necessary to provide a health service,

and

- the third party's information is relevant to the family, social or medical history of that consumer.

See also Principle 1.5 for possible exceptions from notifying an individual where information is collected from third parties.

1.4
If it is reasonable and practicable to do so, the Department of Health and funded service providers must collect personal information about an individual, only from that individual.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Sources of personal information.

Intended privacy protection outcome(s)

Principle 1.4 ensures that the individual maintains control over the way that their personal information is handled by requiring that it should be collected from the individual concerned (except in certain circumstances).

Application of the Principle

We must collect personal information directly from the individual to whom the information relates (or from their authorised representative/agent) where it is reasonable and practicable to do so.

Possible exceptions

There may be situations in which it may not always be 'reasonable' or 'practicable' to collect information directly from the individual. For example, where the **individual is unable** to give or communicate the information, or authorise the collection of information from another person or organisation. This may be because of age, intellectual disability, mental illness, medical condition or some other recognised condition or circumstance.

At times we will have no choice about from whom we collect information, for example if the information arrives **unsolicited**. Where information is unsolicited (that is, where someone passes on information that was not requested), the information is still considered to have been collected if it is either recorded or used, and the individual should generally be notified about this collection. In some circumstances it may not be reasonable to notify an individual about such collections - see Principle 1.5 for possible exceptions from notifying an individual about collection from third parties.

At times collecting information from the individual concerned would **defeat the purpose** of the collection. For example, if information was being collected in order to investigate a breach, or possible breach, of the law.

Other circumstances where information may be collected from third parties is where the collection is **required or authorised by law**. For example, the Child Protection Act requires a person who suspects, on reasonable grounds, that a child has been or is being abused or neglected, to notify the Department of Families and Communities of that suspicion. Collection of that and associated information is a collection that is "required or authorised by law".

Some information about an individual is sought from experts, such as diagnostic tests where information in the form of pathology or radiology results is gathered and added to a patient's file. The implied consent of the individual can be assumed in such collections.

1.5:
Where the Department of Health or funded service provider collects personal information from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed under Principle 1.3 above, except to the extent that making the individual aware of the matter would pose a serious threat to the life or health of any individual.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Notification regarding data collection from third parties and exceptions.

Intended privacy protection outcome(s)

Subject to some exceptions, Principle 1.5 enables the individual to maintain some control over the way that their personal information is handled by requiring that they are informed of all details dealt with in Principle 1.3 when information about them is collected from a third party.

Application of the Principle

This Principle requires us to take reasonable steps to make an individual aware if information about them has been **collected from someone else**. This ensures that the individual is aware of all information collected, regardless of the source of that information.

This Principle applies, unless to inform the individual would pose a serious threat to the life or health of any person (including the individual). For example, if we receive information about an individual who may pose a threat to his or her own life or health, or the lives or health of others, it is reasonable to weigh up whether sharing this advice with the individual concerned would exacerbate the problem. If there is a risk that the situation would be exacerbated, the individual need not be informed.

Possible exceptions

As well as the exception detailed above (where notification would pose a threat to life or health), we would not need to notify an individual about information collected from a third party if advising the individual would **defeat the purpose** of the collection. For example, if information was being collected in order to investigate a breach, or possible breach, of the law.

We are not required to provide a notification when information is being **collected by a third party**, for example, information collected by a party under an outsourcing or contract arrangement. Provided the third party has complied with Principle 1.3, we would not have to do anything more than obtain an assurance from the third party that they have complied with Principle 1.3.

PRINCIPLE 2: USE AND DISCLOSURE

2.1

The Department of Health and funded service providers must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) Both of the following apply:

(i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

and

(ii) The individual would reasonably expect the Department or funded service provider to use or disclose the information for the secondary purpose;

or

(b) The individual has consented to the use or disclosure;

or

(c) If the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) It is impracticable for the Department or funded service provider to seek the individual's consent before that particular use;

and

(ii) The Department or funded service provider will not charge the individual for giving effect to a request by the individual to the Department or funded service provider not to receive direct marketing communications;

and

(iii) The individual has not made a request to the Department or funded service provider not to receive direct marketing communications;

and

(iv) The Department or funded service provider gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications;

or

(d) If the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) It is impracticable for the Department or funded service provider to seek the individual's consent before the use or disclosure;

and

(ii) The use or disclosure is approved by Departmental or Divisional Research and Ethics Committees and the research is conducted in accordance with approved guidelines;

and

(iii) In the case of disclosure - the Department or funded service provider reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;

or

(e) The Department or funded service provider reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) A serious and imminent threat to an individual's life, health or safety;

or

(ii) A serious threat to public health or public safety;

or

(f) The Department or funded service provider has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

or

(g) The use or disclosure is required or authorised by or under law;

or

(h) The Department or funded service provider reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) The enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) The protection of the public revenue;

(iv) The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; and

(v) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: ***It is not intended to deter the Department or funded service providers from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.***

Note 2:	***Sub-clause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in sub-clause 2.1 requires the Department or funded service provider to disclose personal information; the Department or funded service provider is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.***
Note 3:	***The Department or funded service provider is also subject to the requirements of Principle 9 if it transfers personal information to a person in a foreign country.***

EXPLANATORY NOTES

Issue(s) addressed by this Principle

Use and disclosure of personal information.

Intended privacy protection outcome(s)

This principle protects privacy by:

- requiring the Department of Health and funded service providers that hold information about individuals to handle it responsibly, normally by limiting its use to the primary purpose for which it was collected; and
- enabling individuals "to exercise some control over the way information about them is handled" by requiring us, in normal circumstances, to use or disclose information about them only in ways that are consistent with their expectations.

Application of the Principle

This Principle places limits on the extent to which information can be used within the Department and its funded service providers and also limits the circumstances in which information can be disclosed or released to other parties (including other Departments, agencies, organisations or individuals).

"Use" refers to the handling of information *within* a particular organisation.

"Disclosure" refers to the communication of personal information *to* another agency, organisation or individual.

Use and disclosure for the 'primary purpose' of collection – 2.1
When information is collected, it is generally for a specific or 'primary purpose'. Determining the primary purpose of collection should always be possible, although not always easy. When we collect information directly from an individual, it is almost always to serve a specific pre-determined and pre-defined purpose. This is the **primary purpose** of collection. Use or disclosure for any other purpose is a 'secondary purpose' and is dealt with in subsequent paragraphs.

Where the information is *not* collected directly from the individual, our initial use of this information after its collection is a guide to the primary purpose of collection.

Although it is not always necessary for the individual to consent to the use or disclosure of personal information for the primary purpose, we must take reasonable steps to ensure that the individual is aware of the primary purpose – see Principle 1.3.

Use and disclosure of information for a secondary purpose or purpose closely related to the primary purpose of collection – 2.1(a)
This Principle enables the use and disclosure of personal information if that use or disclosure is for a purpose directly related to the primary purpose of collection.

***"*Directly related to the primary purpose"** means a purpose which is closely connected to the purpose for which the information was collected even if it is not strictly necessary to achieve that purpose. For example, a directly related purpose may include:

- managing, evaluating, auditing the provision of a service or product;
- managing the provision of the service or product; and
- administration and/or billing purposes.

However, this Principle requires that the 'secondary use' be within the reasonable expectations of the person to whom the information relates.

The **"reasonable expectations"** test should be applied from the point of view of the general public: that is, we should be able to use or disclose personal information in ways in which a person with no special knowledge of the industry or activity would expect. What a person has been told at the time of collection (in accordance with Principle 1.3) will help to ascertain what an individual might reasonably expect.

Because they are contributing to an individual patient's care, medical students interviewing and examining a patient and reporting findings to a senior doctor and nursing trainees performing procedures on a patient are considered part of the treatment team. In this case, the use of the patient's personal information by (or disclosure to) the student/trainee for the provision of care could be considered a "primary purpose" (but see also the notes to principle 2.1(d) for reference to students who are not part of the treatment team.)

Use and disclosure where the individual has consented – 2.1(b)
Use or disclosure for a secondary purpose is permitted in specified circumstances, including where the individual consents.

"Consent" should be interpreted in a practical way. **"Implied consent"** would be acceptable in some circumstances. Implied consent could legitimately be inferred from the individual's failure to object to a proposed use or disclosure, provided that the option to object was clearly and prominently presented and easy to implement.

However, if serious consequences could arise for the individual from the use or disclosure of information, we would have to be able to demonstrate clearly that every possible effort was made to ensure that the individual understood what was going to happen to his or her information; in such circumstances it would generally be more appropriate to seek **'express consent"**.

In some Aboriginal communities it may be culturally prescribed who may provide consent on behalf of a person. Further information may be obtained from the Aboriginal Services Division of the Department.

Use and disclosure for direct marketing purposes – 2.1(c)
This Principle allows organisations to use non-sensitive personal information for direct marketing where, among other things, it is impracticable to seek the individual's consent and where the individual is told that they can opt out of receiving any more marketing from the organisation.

This Principle only applies to the use of non-sensitive information for direct marketing and does not permit an organisation to disclose personal information for the purpose of direct marketing.

Direct Marketing does not include fundraising in the simple sense of seeking donations. For Health Service providers, collection of name and address to provide a health service would be regarded as the collection of "health information", and as such is specifically not to be used for other purposes without consent (see Principle 10).

Use and disclosure of health information for research purposes – 2.1(d)
Some flexibility is provided by this Principle where **health** information is used or disclosed for the secondary purpose of research or compilation or analysis of statistics relevant to public health or safety.

In general, information used or disclosed for research purposes should be **de-identified**. Where de-identified information is not suitable and it is impracticable to seek consent from individuals, then personal health information may be used or disclosed provided the research has been approved by a Departmental or Divisional Research and Ethics Committee in accordance with NHMRC guidelines issued under S.95A of the Commonwealth *Privacy Act*.

The same principle applies to medical students at a teaching Hospital, who use patient information purely for training purposes and not for any treatment purpose. During activities where students/trainees are not directly involved in an individual patient's care or treatment, wherever possible only de-identified patient information should be used for teaching purposes. Where the use of identifiable patient information purely for teaching purposes is unavoidable and justified, wherever possible, the express consent of the individual patient should be sought. (See also the notes to principle 2.1(a) for situations in which students are part of a treatment team.)

This Principle relates specifically to health information and other provisions apply for using or disclosing other than personal health information (personal information held by housing or community services, for example). Therefore, if personal information which is not health related is required for research purposes, advice should be sought from the Department's Human Research Ethics Committee.

Use and disclosure for health and safety reasons – 2.1(e)
Principle 2.1(e)(i) allows personal information to be used or disclosed to prevent or lessen 'a serious and imminent threat' to the health, welfare or safety of an individual. For this exception to apply, the harm must be about to happen, and the threat to an individual person's health, welfare or safety must be likely to result in significant harm. Where the risk to the health, welfare or safety is remote and unlikely to be prevented or lessened by the release of certain details about an individual, then this exception will not apply and other alternatives for dealing with the situation ought to be considered, for example by seeking consent.

Principle 2.1(e)(ii) allows personal information to be used or disclosed to lessen or prevent a 'serious threat to public health or safety'. This subclause differs from

subclause (i) because it relates to the general 'public health or safety' rather than to an individual's life or safety. Another difference is that 'imminent' has been omitted. This is because a threat to public health or safety, for example, a possible outbreak of infectious disease, may be serious enough to warrant extraordinary uses or disclosures of personal information but may not be imminent in terms of time. It may be certain that, unless addressed, the threat will do serious harm to public health or safety but not certain when that harm will actually be done.

Use and disclosure for investigation and/or reporting unlawful activity – 2.1(f)
This Principle explicitly acknowledges that in some areas of the Department or a funded service provider, the investigation and/or reporting of suspected unlawful activity is a legitimate function. As such, use or disclosure of information is permitted for this purpose.

Use of information for investigating or reporting suspected unlawful activity should be related to our activities or functions. For this to occur, staff will need to be aware of the types of activity that are in breach of statutory requirements.

'Relevant authority' includes law enforcement bodies, such as Police, licensing boards and other government regulatory authorities.

Use and disclosure required or authorised by law – 2.1(g)
This Principle covers situations where the law unambiguously requires or authorises the use or disclosure of personal information, such as legal obligations in relations to notifiable diseases and cases of suspected child abuse.

Use and disclosure for law enforcement purposes – 2.1(h)
Disclosure of personal information to enforcement agencies under Principle 2.1(h) should be confined to information sought in connection with a specific individual case or investigation. Although some enforcement agencies may have legitimate reasons to compile large quantities of data, it is more appropriate for such data to be collected in a more formal and accountable way. Principle 2.1(h) is not intended to justify "fishing expeditions".

In order to rely on this Principle for using or disclosing personal information for law enforcement purposes, staff should 'reasonably believe' that the use or disclosure is reasonably necessary for the law enforcement body to carry out its functions.

For the purpose of this Principle, the term 'law imposing a sanction' would include a law that allows the Government to refuse a benefit or that imposes other non-criminal consequences for failure to comply with a legal obligation.

This clause also acknowledges that we may legitimately use or disclose personal information where necessary for national security reasons. Prejudice to national security would include endangering the defence of Australia or Australia's international relations or information entrusted on a basis of confidence to an Australian government by the government of another country or an international organisation.

2.2
If the Department of Health or funded service provider uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

EXPLANATORY NOTES

Issue(s) addressed by this Principle

Note of personal information used or disclosed for law enforcement purposes.

Intended privacy protection outcome(s)

This Principle enables individuals to exercise some control over the way information about them is handled by requiring a note to be made if personal information is used or disclosed for law enforcement purposes.

Application of the Principle

This Principle requires that on each occasion personal information is used or disclosed for law enforcement purposes (in accordance with Principle 2.1(h)), a note to that effect is created.

Possible exception(s)

The requirement to make a note would not apply where there is a specific statutory provision prohibiting the making of such a record.

2.3
Sub-clause 2.1 operates in relation to personal information that parts of the Department or funded service provider that is a body corporate has collected from a related body corporate as if the Department or funded service provider's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

EXPLANATORY NOTES

Issue(s) addressed by this Principle

Use and disclosure of personal information collected by related body corporates.

Application of the Principle

This Principle aims to ensure that information that we collect from a related body corporate remains subject to the provisions of this Code relating to use and disclosure of personal information.

A related body corporate is defined in Section 50 of the Corporations Act 2001 (Cwth) to mean that where a body corporate is:

- a holding company of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate

the first mentioned body and the other body are related to each other.

2.4
Despite sub-clause 2.1, the Department of Health or funded service providers that provide a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
(a) The individual:
(i) Is physically or legally incapable of giving consent to the disclosure; or
(ii) Physically cannot communicate consent to the disclosure;
and
(b) A natural person (the carer) providing the health service for the Department or funded service provider is satisfied that either:
(i) The disclosure is necessary to provide appropriate care or treatment of the individual; or
(ii) The disclosure is made for compassionate reasons;
and
(c) The disclosure is not contrary to any wish:
(i) Expressed by the individual before the individual became unable to give or communicate consent; and
(ii) Of which the carer is aware, or of which the carer could reasonably be expected to be aware;
and
(d) The disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

EXPLANATORY NOTES

Issue(s) addressed by this Principle

Disclosure of health information to a third party.

Application of the Principle

This Principle recognises that there will be some circumstances where an individual is unable to give consent to the disclosure of his/her personal information but where it may be necessary to contact the individual's guardian, representative, relative or friend and disclose certain health information to ensure that appropriate care or treatment can be provided. Such a disclosure may also be necessary for compassionate reasons, such as telling parents about the condition of an adult child who is unconscious.

Provided all of the following apply, a health provider may disclose health information to someone who is 'responsible' for the individual:

- the individual is physically or legally incapable of giving consent to the disclosure of his/her information or cannot communicate their consent; and

- the disclosure is necessary to provide appropriate care or treatment, or is made for compassionate reasons. The information disclosed must be limited to that which is necessary for this purpose; and
- the disclosure is not contrary to any known wish of the individual.

A definition of those 'responsible' for an individual is contained in Principle 2.5.

Possible exceptions

Disclosures to the media

The media sometimes approach health providers for health information about individuals. For example, where there has been an accident or a crime and the media is interested in the nature and extent of any injuries or a negligence claim against a hospital about which the media want to do a public interest story.

There is no provision under Principle 2 for disclosing information to the media unless the individual has consented. As a result, where no consent has been given, a health provider should only release information that would not identify the individual, or allow them to be identified from the details or context or situation. For example, a generic statement to the effect that "an elderly gentleman involved in an accident is in a serious condition" may be acceptable. Detailed medical information must not be disclosed.

2.5
For the purposes of sub-clause 2.4, a person is responsible for an individual if the person is:

(a) A parent of the individual;
or
(b) A child or sibling of the individual and at least 18 years old;
or
(c) A spouse or de facto spouse of the individual;
or
(d) A relative of the individual, at least 18 years old and a member of the individual's household;
or
(e) A guardian of the individual;
or
(f) Exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;
or
(g) A person who has an intimate personal relationship with the individual;
or
(h) A person nominated by the individual to be contacted in case of emergency;
or
(i) a person defined by traditional Aboriginal law.

2.6
In sub-clause 2.5:
child **of an individual includes an adopted child, a step-child and a foster-child, of the individual.**

parent **of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.**

relative **of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.**

sibling **of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.**

PRINCIPLE 3: DATA QUALITY

3
The Department of Health and funded service providers must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Data quality.

Intended privacy protection outcome(s)

This principle:

- places the onus on us to keep any information we hold up-to-date, accurate, complete and not misleading; and
- reinforces the right of an individual to seek amendment of their personal information if it is found to be incorrect (see Principle 6).

Application of the Principle

We should, prior to using personal information, take reasonable steps to ensure that it is accurate, complete, up-to-date and not misleading.

In some circumstances, we will rely on individuals to keep information up-to-date, such as an individual's name or address. It is our responsibility to advise people of their obligations in this regard.

Possible exceptions

This Principle does not require us to maintain the quality (accuracy, completeness and currency) of personal information throughout the entire duration that we hold the information. There is no obligation to check the quality of personal information when it is not currently in use.

However, there are risks associated with the use or disclosure of archived personal information that has not been recently checked for its quality. Hence, we should take reasonable care to ensure the quality of personal information when it is collected, used or disclosed.

PRINCIPLE 4*:* DATA SECURITY

4.1
The Department of Health and funded service providers must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Data security.

Intended privacy protection outcome(s)

This Principle aims to protect the security of personal information in our possession.

Application of the Principle

This principle places an obligation on us to ensure that any personal information we hold is kept **secure**.

The Department or any funded service provider that holds personal information must take 'reasonable steps' to ensure that any personal information it holds is protected against threats of:

(a) loss;
(b) inadvertent access, destruction, use, modification or disclosure; *and*
(c) any other misuse.

What are 'reasonable steps'?
In determining what is "reasonable" the safeguards should be appropriate to the sensitivity of the personal information being stored or transmitted. Some information, such as medical records, financial details, information dealing with child protection or mental health, will always be deemed highly sensitive and require high levels of protection. It should be noted that any information can be sensitive, depending on the context in which it is used. For example, in circumstances involving domestic violence orders, individuals directly involved may consider their residential address to be highly sensitive warranting appropriate safeguards to ensure its security.

When determining the level of effective safeguards that are appropriate to the sensitivity of information involved, requirements to implement safeguards should take account of the cost of implementing such safeguards.

Methods for safeguarding security could include*:*

(i) **Physical measures**, for example, locked filing cabinets, clear desk policies and restricted access to offices;

(ii) **Organisational measures**, such as providing access to information only on a 'need-to-know' basis;

(iii) **Training measures**, including making sure staff are adequately trained in the handling of personal information in accordance with this Code and other legislative requirements; and

(iv) **Technological measures**, for example, the use of passwords, lockable screen savers, firewalls and encryption.

Responsibilities of third parties

Where personal information is provided to a third party, we should ensure that security measures are implemented. For contractors, sub-contractors or fee-for-service professionals, contracts should contain clauses which state that the privacy protection principles in this Code set the minimum standards for the handling of personal information, including safeguards to protect its security. For others with access to personal information, for example researchers, signed undertakings can be a means of ensuring that any information released will be protected.

4.2
In accordance with the provisions of the State Records Act, 1997, the Department of Health or funded service provider should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under Principle 2.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Data security and quality.

Intended privacy protection outcome(s)

This Principle aims to protect the security of personal information in our possession by requiring that personal information be destroyed or permanently de-identified in accordance with the State Records Act once no longer required or used.

Application of the Principle

There are significant risks and costs associated with the long-term storage of personal information. We can effectively minimise exposure to these risks and information management overheads by implementing systems for the methodical destruction or de-identification of personal information for which there is no future intended use (including future historical use).

This Principle acknowledges that much of the information we collect will form part of an 'official record' under the State Records Act. '**Official record**' means a record made or received by an agency in the conduct of its business. As a result, this Principle gives no authority nor is it a mandate to destroy information. Destruction (or disposal) of an official record may only be carried out in accordance with a determination made by the Manager of State Records with the approval of the State Records Council.

PRINCIPLE 5: OPENNESS

5.1
The Department of Health and funded service providers must set out in a document clearly expressed policies on its management of personal information and must make the document available to anyone who asks for it.

5.2
On request by a person, the Department of Health or funded service provider must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Maintaining a policy of openness.

Intended privacy protection outcome(s)

This principle ensures that the information we hold about individuals is handled responsibly by promoting openness, transparency and accountability in the manner in which we handle personal information.

Application of the Principle

This principle requires us to be open about what kinds of personal information we hold and what we do with that information. We must make available to our clients, information about the policies and procedures we use to manage personal information. We should also provide access to copies of this Code upon request. Providing access to such policies should be undertaken in accordance with the provisions of the Freedom of Information Act, 1991 (ie the policy itself should not contain any 'exempt' material – see the Freedom of Information Act (FOI Act) for further details about 'exempt' material).

We could employ a range of communication strategies to inform individuals of:

- the means of gaining access to personal information held (in accordance with Principle 6 and the FOI Act);

- a description of the type of personal information that is under our control and a general account of its use (refer Principle 1.3); and

- the title and address of the person who is accountable for our policies and practices for handling personal information and to whom complaints and/or enquiries regarding these policies and practices can be directed (refer Principle 1.3).

The means of communicating this information could include:

- preparing pamphlets, flyers, information sheets, etc;
- providing details on our web site; and
- including these additional details in our FOI Information Statement, annual report, etc.

In relation to Principle 5.2, it is intended to generally cover the broad types of personal information we hold and how we handle that information. The obligation to provide a particular individual with access to their information is covered under Principle 6.

PRINCIPLE 6: ACCESS AND CORRECTION

6.1
Where the Department of Health or funded service provider has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the Department or funded service provider is required or authorised to refuse to provide the individual with access to that record under any law.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Access to personal information.

Intended privacy protection outcome(s)

This principle enables an individual to discover and access information that we hold about them.

Application of the Principle

The right of access to personal information is a very important privacy right and Principle 6.1 provides that, **wherever possible**, we should permit individuals to see the personal information that we hold about them.

However, in doing so, this Principle also recognises that there are legislative provisions which provide for access, or refusal of access, to personal information which override the provisions of this Code. For example, the *Freedom of Information Act* provides a legally enforceable right of access to any document in the possession of the Government, or to which the Government has a ready right of access. Despite this right, the FOI Act also authorises and, in some instances, requires an agency to deny access to certain types of documents.

There are also other legislative provisions which may require an agency to refuse access to certain types of information even if it contains personal information. These provisions include those in the *Child Protection Act*, which requires that any information which would lead to the identity of a notifier must not be disclosed or released.

Therefore, the provisions of this Code do not oblige us to provide access to any document which would otherwise be denied under any legislative provision.

Despite any other legislative provision, to give effect to this Principle, we may wish to consider implementing a less formal policy providing access to certain types of personal information which are known to be readily available (ie where there is no doubt that the information is not exempt from release under any other Act). If no such open access policy exists, the FOI Act will generally apply.

Information held by a non-government organisation

If a non-government organisation holds information about an individual as a result of an arrangement with the Department of Health, the individual can approach the Department regarding access to that information.

For this reason, it is important that any contract, agreement or arrangement between the Department of Health and a contractor, consultant, researcher, private agency, etc, contains provisions which enable it to access information generated or held because of that contract, agreement or arrangement. This will ensure that the Department has a ready right of access to the information, and, as a result, an individual will maintain their legal right of access to the information under the FOI Act.

The Department will also need to ensure that, in any contract, agreement or arrangement, where it provides or transfers information to a third party to enable that party to undertake a function for, or on behalf of, the Department, the transfer does not constitute 'disposal'[2] under the State Records Act.

[2] Under the State Records Act 1997, “dispose of” an official record includes “transfer or deliver ownership or possession of or sell the record, or purport to do so” but does not include to transfer or deliver the record to State Records or between one agency and another.

6.2
Where the Department of Health or funded service provider has possession or control of a record that contains personal information, the Department and funded service provider should take such steps (if any), that are, in the circumstances, reasonable to amend a record that is not accurate, complete or up-to-date, except to the extent that the Department or funded service provider is required or authorised to refuse to amend a record under any law.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Correction of personal information

Intended privacy protection outcome(s)

This Principle endeavours to ensure that all decisions are based upon personal information which is current, complete and correct. The right to correct personal information also gives individuals confidence in the quality and integrity of the personal information we hold.

Application of the Principle

Principle 6.1 requires us to take all reasonable steps to ensure that the personal information we hold is of high quality. This is because decisions which are based on poor quality information may have adverse consequences for the individual.

Therefore, prior to using personal information, we should take steps to ensure that it is accurate, complete, up-to-date and not misleading (see also Principle 3 dealing with Data Quality). In some circumstances, we may need to rely on individuals to keep their information up-to-date, such as the individual's name or address which can often be subject to change. It is our responsibility to advise people of their obligations in this regard and to have simple and accessible mechanisms to assist individuals to keep their information up-to-date.

“Reasonable steps” imply that, if the personal information is shown to be of poor quality but is inaccessible and will never be used, then we would not be obliged to expend resources correcting information that is unlikely to be used. Nevertheless, in accordance with Principle 4 that deals with data security, storing poor quality personal information reflects a poor standard of information management and is consequently most undesirable. Hence, ‘reasonable steps’ needs to be broadly interpreted.

This Principle also recognises that there are legislative provisions which may provide for correction or amendment of personal information (the Freedom of Information Act, for example). Like Principle 6.1, such provisions, due to their legislative nature, will override the provisions of this Code. As such, other than routine updating of information (for example, telephone and addresses) the FOI Act will generally apply.

However, it should be noted that under the FOI Act, where an agency refuses to amend a record, the individual may request a notation to be put with the record. As a result, when considering new systems for holding information, particularly in an electronic environment, it is important to consider how a notation can be accommodated. The addition of a "comments" field can sometimes serve this purpose.

Upon request, we should, under normal circumstances, inform the individual whether or not we hold personal information about them. When doing so, we should also notify the individual of the mechanisms in place to facilitate access to this information and how they may request correction of the information. This supports Principle 5 which requires a policy setting out details of personal information handling practices.

Possible exceptions

In some situations, it might be necessary for us to keep a record of what we knew or understood at a particular time - the information a particular decision was based upon - which would require the retention of information that was incorrect, out-of-date, or misleading. Legislative provisions (for example, the Evidence Act) may also require that such information be retained.

PRINCIPLE 7 UNIQUE IDENTIFIERS

7.1
The Department of Health and funded service providers must not adopt as its own identifier of an individual, an identifier of the individual that has been assigned by:
(a) The Department of Health or funded service provider; or
(b) an agent of the Department or funded service provider acting its capacity as agent; or
(c) a contracted service provider for a Department of Health or funded service provider contract acting in its capacity as contracted service provider for that contract; or
(d) a Commonwealth Government agency, its agent, or its contracted service provider
Unless:
(a) The use or disclosure is necessary for the Department or funded service provider to fulfil its obligations; or
(b) The use or disclosure is permitted under Principle 2.1

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Unique **identifiers**.

Intended privacy protection outcome(s)

This limits the use of the same unique identifier across different organisations and thereby minimises the likelihood of personal data being misused or shared in an inappropriate manner.

Application of Principle

Government agencies and non-government organisations widely use identifiers to keep track of information they hold about individuals. Most organisations are likely to have one or more systems in place that rely on identifiers.

While the assignment of a unique identifier does not in itself raise privacy issues, the way in which this identifier is used (or could be potentially used) may raise concerns. For example, while some of the benefits of unique identifiers are in checking for duplication errors in the data held about individuals as well as facilitating the linking of client-specific information from different data sources, they represent a potential threat to privacy by facilitating more ready access to personal information held throughout the organisation in different data stores. Consequently, strict criteria should apply to the initial assignment of unique identifiers (ensuring that it is necessary for a particular purpose) and limitations should be placed on their subsequent use. These safeguards will minimise the likelihood of personal data being misused or shared in a manner that is inappropriate.

Unique identifiers can also be used to facilitate the easier sharing of information between divisions of the Department or funded service providers, but only where this is considered necessary to enable them to carry out a particular function or activity, and where this activity is carried out in accordance with this Code.

This Principle aims to ensure that an identifier assigned for a particular function or activity does not become more generally adopted and used as an identifier for a whole range of other unrelated functions and activities and, by stealth, become a kind of universal identifier. This Principle should apply regardless of where the identifier originated. For example, it could be an identifier generated by a government or division of government (either State, Local or Federal) or a non-government organisation.

What is an identifier?

An 'identifier' includes a number assigned to an individual to uniquely identify the individual to enable an organisation to perform its functions. An identifier can be numbers, letters or both, but is not limited to numbers or letters. For example, widely known identifiers include an individual's medicare number and drivers licence number. An individual's name and address is not, of itself, however considered to be an 'identifier'.

Because it is sometimes necessary or more efficient to assign an identifier, reasonable steps should be taken to ensure that a unique identifier is assigned only to an individual whose identity has been clearly established through reference to other collaborative information.

Use of an identifier necessary to fulfil obligations

Care is required when assigning and using unique identifiers to ensure that the standards established in this Code are met. In particular Principle 2 concerning use and disclosure of personal information which requires that information collected for one purpose generally should not be used or disclosed for an unrelated purpose, unless the individual consents, or there is a legal requirement or authorisation to do so, or another exception under Principle 2 applies.

It should not be compulsory for an individual to provide a unique identifier in exchange for a service unless the identifier is connected to that purpose (or a directly related purpose) for which it was assigned or unless this is required or authorised by law. For example, it is necessary for an individual to provide their Medicare number in certain health care situations for billing purposes. However, if the Medicare number is requested when the individual is seeking an unrelated service, then it should be up to the individual whether they wish to supply their Medicare number, and they should not experience any disadvantage if they choose to refuse.

This Principle prevents us from requesting government-assigned identifiers for all of the individuals with which we deal, and using these identifiers to organise the personal information that we hold and/or to match this personal information with other information by reference to the same unique individual identifiers (unless otherwise authorised to do so).

Possible exceptions

Necessity of recording an identifier assigned by some other body
There are times when it is necessary for us to record identifiers which have been assigned by another division, department, government or organisation.

For example, while Medicare numbers are required for billing purposes in relation to health services, it should not be used as the basis for another organisation's own identification system.

Similarly this principle would not stop us collecting and recording government-assigned unique identifiers to establish or verify the identity of the individuals they are dealing with. However, unless required to do so, when evidence of individual identification is required or authorised (including by law) such as a 100-point identity requirement, consideration should be given to whether it is necessary to record the identifier. In some situations it may be sufficient to simply sight the drivers license or other form of identification.

PRINCIPLE 8: ANONYMITY

8
Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with the Department of Health and funded service providers.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Anonymity of individuals.

Intended privacy protection outcome(s)

This Principle enables an individual to exercise some control over the way his/her personal information is collected, by allowing (where possible), an individual to deal anonymously with us.

Application of the Principle

Anonymity is an important mechanism of privacy protection. Its significance has increased in response to the increased use and capabilities of technology, including data matching and electronic surveillance, which enable an individual's activities to be monitored.

This Principle supports the reasonable expectation of individuals that they can choose to conduct their lawful day-to-day activities without being required to identify themselves. However, the application of this Principle is not intended to, nor must it, facilitate illegal activities.

There are a number of circumstances in which an individual should be able to remain anonymous, for example in the collection and analysis of client surveys in which collective statistics are used to demonstrate conclusions or trends but where no identifiable information is required.

Possible exceptions

In some circumstances, it will not be practicable to deal with individuals anonymously. In others, there will be legal obligations that prohibit anonymous dealings with individuals. This Principle is intended to enable individuals the option to operate anonymously unless there is a good practical or legal reason to require identification.

PRINCIPLE 9: TRANSBORDER DATA FLOWS

9
The Department of Health and funded service providers must not transfer personal information about an individual to someone (other than the Department or funded service provider or the individual) unless:

(a) The Department or funded service provider reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to Principles contained in this Code;

or

(b) The individual consents to the transfer;

or

(c) The transfer is necessary for the performance of a contract between the individual and the Department or funded service provider, or for the implementation of pre-contractual measures taken in response to the individual's request;

or

(d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Department or funded service provider and a third party;

or

(e) All of the following apply:

(i) The transfer is for the benefit of the individual;*and*

(ii) It is impracticable to obtain the consent of the individual to that transfer; *and*

(iii) If it were practicable to obtain such consent, the individual would be likely to give it.

or

(f) The Department or funded service provider has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Principles contained in this Code.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Security of personal information during transmission.

Intended privacy protection outcome(s)

This principle requires us to ensure that information is protected from misuse, loss and unauthorised access, modification or disclosure during transmission.

The principle is consistent with the restrictions on international transfers of personal information described in the European Union Directive 95/46.

Application of the Principle

This principle is aimed at ensuring information that is transferred to another body remains subject to effective privacy protection. It recognises that, to fulfil certain functions, we may need to disclose/transfer information to another: division of the Department; funded service provider; government; non-government organisation; or individual. For example information may need to be transferred/disclosed: to provide a service or undertake a function: for research purposes; to enable a funded service provider or non-government organisation to undertake a function for, or on behalf of, the Department; for participating in national initiatives; or for the purpose of fulfilling a legislative requirement.

This Principle requires us to ensure that, during transmission, personal information is safeguarded in a way that is consistent with this Code - that is, it is safeguarded from unauthorised access, misuse and loss. This also applies to other organisations in the event that these bodies subsequently disclose information to another external party. Clauses reflecting this responsibility should be included in all agreements, contracts and undertakings with other organisations and individuals when personal information is transferred.

Methods of securing information during transmission

There are many different ways of securing personal information during its transmission to another section of the Department or funded service provider or to a third party. Reasonable steps should be taken to avoid unnecessarily transmitting personal information across public networks, by fax, e-mail or other unsecured mediums, especially if the transmission is in plain text or includes sensitive information.

Ways to secure information during transmission include the use of adequate encryption technology, advising fax recipients in advance that a message containing personal information is being sent or considering whether de-identified information will be adequate for the recipient. For example, for some research projects it may not be necessary for the researcher to be provided with identifiable information.

PRINCIPLE 10: SENSITIVE INFORMATION

10.1
The Department of Health and funded service providers must not collect sensitive information about an individual unless:

(a) The individual has consented;

or

(b) The collection is required or authorised by law;

or

(c) The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) Is physically or legally incapable of giving consent to the collection;

or

(ii) Physically cannot communicate consent to the collection;

or

(d) If the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) The information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) At or before the time of collecting the information, the Department or funded service provider undertakes to the individual whom the information concerns that the Department or funded service provider will not disclose the information without the individual's consent;

or

(e) The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Collection of **sensitive** personal information.

Intended privacy protection outcome(s)

This principle:

- reinforces the Principle that only necessary information be collected;
- acknowledges that certain sensitivities are attached to some types of personal information; and
- recognises the benefits of collecting and using sensitive personal information for public health, safety and welfare reasons.

Application of the Principle

This Principle places limits on the collection of **sensitive** information about individuals.

What is "sensitive" information?
"**Sensitive**" information includes information revealing political opinions, religious beliefs, trade union membership, or details of health or sex life.

Specific requirements relating to the collection of "**health information**" are outlined below.

Collection of sensitive personal information where the individual consents – 10.1(a)
This Principle acknowledges that consent from an individual would cover practically all legitimate uses or disclosures of the above categories of sensitive personal information. For example, a person who identifies themselves to us as having a particular religious affiliation so that he or she may be treated in a culturally appropriate manner could be assumed to consent to the information being retained for future dealings.

Other examples include where a sample is sent to a pathology laboratory or an individual is transferring to another organisation. In these instances, we could rely on the implied consent of the individual for us to collect and use laboratory results, and to disclose sensitive personal information to a recipient organisation.

Collection of sensitive personal information required or authorised by law – 10.1(b) AND 10.2(b)
There are some laws which require or authorise the collection of sensitive personal information. For example, the *Public And Environmental Health Act* requires the Health Commission to collect information regarding notifiable diseases. Similarly, the *Children's Protection Act* authorises the Department of Health to collect information, including sensitive personal information, relating to an alleged case of child abuse.

Collection of sensitive personal information necessary to prevent or lessen a serious threat to life or health - 10.1(c)
This Principle applies in cases where an individual is incapable, due to physical or legal reasons, to consent to the collection of sensitive personal information if that information is required to prevent or lessen a serious and imminent threat to the life or safety of any individual. Medical emergencies is a typical example of where this Principle would be relied upon to collect sensitive personal information without the individual's consent such as where a person is unconscious as a result of a stroke. The hospital may wish to contact the individual's GP for advice about his/her medical history and medication regime. Where this information is necessary to lessen the threat to the life or health of the individual, this Principle supports the common law duty of care and does not prohibit the hospital from collecting that information.

This Principle also supports cases where the Department is investigating an alleged case of child abuse. In some circumstances it may be necessary to collect sensitive personal information about the alleged victim or alleged abuser, without the consent of that person (or their parent or guardian).

Collection of sensitive personal information necessary for organisational membership – 10.1(d)

If a Division of the Department or a funded service provider has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims, this Principle enables it, in the course of its activities, to collect sensitive information about a member or a person in regular contact with it, provided that it undertakes to the individual that it will not disclose this information without the individual's consent.

Collection of sensitive personal information necessary to establish, exercise or defend a legal or equitable claim - 10(1)(e)

This Principle does not prohibit us, in the preparation of a court case, to collect sensitive information about a client or about the parties or witnesses without getting their consent if that information is necessary to conduct the case.

Possible exceptions

Compliance with national agreements may require the collection of sensitive information. For example, the National Health Information Agreement which establishes the funding guidelines to support Medicare may require data collections to identify ethnicity in order to demonstrate any racial inequities in access to services.

10.2
Despite subclause 10.1, the Department of Health or funded service provider may collect health information about an individual if:

(a) The information is necessary to provide a health service to the individual;
and
(b) The information is collected:
(i) As required or authorised by law;
or
(ii) In accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the Department of Health or funded service provider.

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Health information.

Intended privacy protection outcome(s)

This principle:
- reinforces the Principle that only necessary information be collected; and
- acknowledges that the collection of certain information is necessary to provide a health service.

Application of the Principle

Principle 10.2 requires that health information only be collected if it is necessary to provide a health service to an individual and when that information is collected in accordance with law or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality.

Information necessary to provide a health service – 10.2(a)
Like Principle 1.1, this Principle requires that information collection should be limited to that which is necessary - in this instance necessary to provide a health service. Generally, if information is not needed or is irrelevant for a particular purpose, then it should not be collected.

While it may not be immediately obvious, in many cases it will be necessary for a health service provider to collect all the medical history he/she can. This information may be required in order to provide a quality health service and to cover any legal liability obligations a health provider may need to take into account.

However, this Principle aims to limit situations where unnecessary information is collected unintentionally or where too much information is collected. For example, a hospital may have a form with spaces to collect a lot of standard information, particularly where the form serves a number of purposes. Most people feel that they have to fill in all fields unless they are informed otherwise. By letting people know what information is necessary/mandatory/most relevant to their situation, it is possible to minimise the collection of unnecessary information.

In addition to limiting health information collection to that which is necessary to provide a health service, this Principle requires that this collection be undertaken as required **or** authorised by law or in accordance with rules issued by competent health and medical bodies which are discussed below.

Collection of health information required by law – 10.2(b)(i)
Principle 10(2) enables personal health information to be collected in order to provide a health service provided the collection is required by law. For example, the *Mental Health Act 1993* enables the Director of a treatment centre to collect information concerning a person from a psychiatrist who has made an order for the detention of that person.

See also Principle 10.1(b)

Collection in accordance with rules established by competent health or medical bodies – 10.2(b)(ii)
If collection of health information is necessary to provide a health service but the collection is not required or authorised by law, the collection must be undertaken in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

The types of bodies that generally deal with obligations of professional confidentiality, include those bodies which are established under law to register or regulate health professionals (the Medical Board and Dental Practitioners Board, for example).

10.3
Despite Principle 10.1, the Department of Health and funded service providers may collect health information about an individual if:

(a) The collection is necessary for any of the following purposes:
- **(i) Research relevant to public health or public safety;**
- **(ii) The compilation or analysis of statistics relevant to public health or public safety;**
- **(iii) The management, funding or monitoring of a health service;**

and

(b) That purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;

and

(c) It is impracticable for the Department or funded service provider to seek the individual's consent to the collection;

and

(d) The information is collected:
- **(i) As required or authorised by law;**
- **(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the Department or funded service provider;**
- **(ii) in accordance with Departmental or Divisional Research and Ethics Committee approval**

EXPLANATORY NOTES

Issue(s) addressed by the Principle

Collection of **health information** for research purposes

Intended privacy protection outcome(s)

This principle imposes certain conditions on the collection of personal health information for research purposes.

Application of the Principle

Principle 10.3 provides some flexibility for the **collection** of health information for research that is relevant to public health and safety and when health information is used for managing a health service.

When collection of de-identified information is not suitable for the research or management purposes, and it is impracticable to seek the individual's consent to the collection, then so long as certain procedures and guidelines are followed, identifiable health information may be collected, for research and management purposes.

See Principle 2 for **use and disclosure** of health information for research purposes, "primary purposes", "directly related" and "secondary" purposes.

Collection necessary for research or compilation or analysis of statistics relevant to public health or public safety or for the management, funding or monitoring of a health service – 10.3(a)
This Principle enables us to collect health information for research or for the compilation or analysis of statistics relevant to public health or public safety.

What is 'relevant' to public health or public safety?
This Principle recognises that the collection of identifiable health information (without the consent of the individual concerned) for research or statistical purposes may benefit public health or public safety.

To use this Principle as a means of collecting health information, the research or the compilation or analysis of statistics must be relevant to public health or public safety. To be "relevant", the outcome of the research or the statistics must impact on or provide information about public health and safety. For example, this could include research about the impact of a polluted waterway on the health of those living around it, national statistics on breast cancer or statistics on diabetes as a cause of death.

What is "management, funding or monitoring of a health service"?
Examples of collection for the management, funding or monitoring of a health service which are applicable for the purpose of this Principle might include:

- a quality assurance body collecting data about the quality of health service provided
- an external body collecting information about adverse events in hospitals; or
- collection of health information to investigate the possibility of fraud or incorrect payments.

Where the purpose cannot be served by de-identified information – 10.3(b)
This Principle requires detailed consideration of whether de-identified information could be used for research, statistical or management purposes.

De-identified health information may not always achieve a particular purpose, such as where a project involves linking information about individuals from two or more sources and identified information might be needed to correctly link the data. However, when identifying information is required, consideration should be given as to whether it is necessary to store it in the identified form. For example, once data is linked (as described above), consideration should be given to whether it is necessary to keep the identified information or whether at this stage the information could be de-identified.

Where it would be impracticable to seek consent – 10.3(c)
In deciding whether it would be impracticable to seek consent of individuals for the collection of health information for research, statistical or management purposes, a number of factors may need to be taken into consideration. For example, these may include: the age of the information and whether the address is likely to be current; or whether there is sufficient information to identify particular individuals in order to gain consent (ie name and address may not always be sufficient to identify a particular individual). Time and cost are not always factors in the decision about whether seeking consent is impracticable.

Collection required or authorised by law – 10.3(d)(i)
Collection of health information may be required by law for research, statistical or management purposes such as when collection is required under an Act including Committee's established under S.64D of the *Health Commission Act* and reporting notifiable diseases.

Collection in accordance with rules established by competent health or medical bodies – 10.3(d)(ii)
See 10(2(b)(ii) for details of "competent health or medical bodies".

Collection in accordance with Departmental or Divisional Research and Ethics Committee approval – 10.3(d)(iii)
This Principle acknowledges the role that Departmental and Divisional Human Research and Ethics Committees play in assessing research proposals and setting out the criteria under which proposals will be approved.

Principle 10.3(d) requires any collection of identifiable health information for research or statistical purposes (where it is not practicable to obtain consent and the purpose cannot be served by de-identified information) to be approved by a Human Research and Ethics Committee. Such approvals should be undertaken in accordance with guidelines issued by the National Health and Medical Research Council and, in particular, those guidelines issued under Sections 95 and 95A of the Commonwealth Privacy Act.

10.4
If the Department of Health or funded service provider collects health information about an individual in accordance with subclause 10.3, the Department or funded service provider must take reasonable steps to permanently de-identify the information before the Department or funded service provider discloses it.

10.5
In this clause *non-profit organisation* means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

APPENDIX A

DEFINITIONS OF KEY TERMS

Access
In Principle 6 "access" refers to an individual's right of access to information in accordance with the Freedom of Information Act, 1991.

Authorised by law
"Authorised by law" refers to circumstances where the law permits, but does not require, the use, disclosure, or denial of access to, personal information. The word "authorised" suggests that there is some discretion as to whether or not to use or disclose or deny access to information (see Principles 2.1(g) and 6.1(j)).

Collection
We collect personal information if we gather, acquire or obtain information from any source, by any means, in circumstances where the individual is identified or is identifiable. It includes information that:

- we come across by accident or has not asked for but nevertheless keeps;
- information we receive directly from the individual; and
- information about an individual we receive from somebody else.

Department
Department means the South Australian Department of Health.

Direct marketing
Direct marketing includes activities that promote the sale or purchase of products or services or promote charitable fundraising where the individual is approached directly. It includes in-person approaches to people's houses and approaches by mail, e-mail, telex, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy services at a distance (for example to buy by phone, mail or website) or to visit retail and service outlets or to donate to a cause by one of these means. It also includes automated processes such as Spam e-mail and computer generated voice calls over the phone.

Directly related purpose
A directly related purpose is one that has a strong connection with the primary purpose of collection. It is closely associated with the original purpose, even if it is not strictly necessary to achieve that purpose. Uses or disclosures for a directly related purpose would include uses or disclosures for:

- monitoring, evaluating, auditing the provision of the particular product or service we have or are providing to the individual;
- managing the provision of the service or product;
- following up complaints about the service or product;
- administrative purposes associated with providing, following up on or receiving payment for the service or product; and
- reminders where an individual receives a service on a regular basis.

See also Primary Purpose, Related Purpose and Secondary Purpose.

Disclosure
We disclose information when we release information *outside* the Department or its funded service providers. Examples of disclosures include:

- when we give another Department, Government, organisation or individual information under contract to carry out an "outsourced" function;
- when we sell information to another organisation.

Employee record
An employee record includes personal information *about the employment of* an employee.

Personal information relating to an employee's employment may include health information about them.

Other personal information about the individual and their employment, which might also be held in an employee record, includes information about:

- their engagement, training, disciplining or resignation;
- their termination of employment;
- the terms and conditions of their employment;
- their personal and emergency contact details;
- their performance and conduct;
- their hours of employment;
- their salary or wages;
- their membership of a professional or trade association;
- their trade union membership; and
- their leave, including recreation, long service, sick, personal, maternity and paternity leave; and
- their taxation, banking or superannuation affairs.

Enforcement bodies
Enforcement bodies referred to in Principle 2.1(h) includes:

- the Australian Federal Police;
- the National Crime Authority;
- the Australian Customs Service;
- the Australian Prudential Regulation Authority;
- the Australian Securities and Investments Commission;
- State, Federal, and Territory agencies responsible for administering or performing a function under a law that imposes a penalty or sanction;
- State, Federal, and Territory agencies responsible for administering a law relating to the protection of public revenue;
- State or Territory police services;
- State and Territory authorities responsible for conducting criminal investigations or inquiries.

Health information
Health information means information or an opinion that is also personal information about the:

- health or disability (at any time) of an individual;
- individual's expressed wishes about the future provision of health services;
- health services provided or to be provided to an individual that is also personal information or other personal information collected to provide, or in providing a health service;
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

Health information can include details such as an individual's name, address, billing information and Medicare number, for example, if it is part of the information about an individual's health.

Health service
Health service means an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual, or the person performing it, to:

- assess, record, maintain or improve the individual's health;
- diagnose the individual's illness or disability;
- treat the individual's illness or disability or suspected illness or disability; or
- dispense on prescription a drug or medicinal preparation by a pharmacist.

Individual
The word "individual" used in this Code relates to the person whose personal information we hold. The words "person" or "people" are used when referring to anyone other than the individual.

Law
The reference to law in this Code means State, Commonwealth, and Territory legislation as well as the common law.

Lawful
Lawful means something that is not prohibited by law. This is a wider concept that "authorised by law" or "required by law".

Necessary
If we cannot, in practice, effectively pursue a function or activity without collecting personal information, then that personal information would be regarded as "necessary" for that function or activity. Necessary should not be interpreted as a reason for collecting information on the off chance that it may be useful for a function or activity in the future.

Personal information
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.

Personal information must relate to a *natural* person. A natural person is a human being rather than, for example, a company, which may in some circumstances be recognised as legal "person" under the law.

Personal information can range from the very sensitive (for example, political beliefs, medical history, sexual preference or medical records) to the everyday (for example, hair colour, address, phone number). The information need not be accurate, it may include opinion and speculation and it may simply be false information. It doesn't matter whether the information is held in a computer database, or in paper records, or in any other medium. If the information itself makes it clear which individual it is about then the individual is identifiable. Whether an individual's identity is reasonably ascertainable will depend on the context and on who holds the information.

Practicable and impracticable
What is practicable or impracticable involves assessing the facts of the particular situation. It is not determined by an individual's, or an organisation's view of what is practicable or impracticable. Something would not generally be considered as impracticable just because it involves expense, inconvenience or effort. (for example, see Principles 1.3, 1.4, 2.1(c) and (d), 8 and 9).

Primary purpose
The primary purpose is the dominant or fundamental reason for information being collected in a particular transaction.

There can only be one primary purpose of collection for a particular transaction. When an individual gives (and we collect) personal information, we and the individual almost always do so for a particular purpose, for example, to receive a service. This is the primary purpose of collection, even if we have some additional purposes in mind. These additional purposes will always be secondary purposes for that transaction, even if we tell the individual about them, and even if the individual's consent is gained to use or disclose the information for those additional purposes. For more information about primary purpose see Chapter 4 – Collecting personal information.

See also directly related purpose, related purpose and secondary purpose.

Reasonable
The terms "reasonable" and "unreasonable" appear frequently throughout this Code. Generally speaking, they relate to decisions or steps to be taken in particular circumstances (for example, when collecting, or using and disclosing information) or to expectations of individuals in those circumstances.

Determining what is reasonable involves considering the factual circumstances in which we are acting rather than the individual's or our view of what is reasonable or unreasonable. (See Principles 1.2, 1.3, 1.5, 2.1)d(3), 2.1(h), 3, 4, 5.2, 6.1(c), 6.3, 6.5 and 9(f).)

Record
A record is "anything in which information is stored or can be reproduced" (FOI Act).

It can include a document, a database, a photograph, picture, x-ray or specimen results.

Related corporation
The question of whether one corporation is related to another corporation is determined in the same way as it is determined under the Corporations Law. This means that where a body corporate is:

- a holding company of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate.

the first mentioned body and the other body are related to each other.
(From Corporations Law- Section 50)

Related purpose
A related purpose includes all the purposes that are directly related purposes as well as some additional ones. Related purposes must have some connection to, and arise in the context of, the primary purpose. Uses or disclosures for a related purpose would include uses or disclosures:

- giving a person information closely associated with a particular product or service an individual receives from us; or
- notifying an individual who has received a service or product from us in the past of a business change of address.

See also directly related purpose, primary purpose and secondary purpose.

Required by law
Required by law refers to circumstances where a law requires the collection, use or disclosure or denial of access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offence. Such a law may specifically require an organisation to collect, use, disclose or deny access. It may also be a law that gives another body a general information gathering power. (see Principles 2.1(g), 6.1(h), 10.1(b)).

Secondary purpose
Secondary purposes are purposes other than the primary purpose that the we have in mind for the information we collect. Related and directly related purposes are secondary purposes.

We must not use or disclose information for secondary purposes except in limited circumstances, such as where we have the consent of the individual, or where the secondary purpose is related or directly related and within reasonable expectations. Principle 2 allows very limited unrelated secondary use for the purpose of direct marketing where it is impracticable to get consent.

See also directly related purpose, primary purpose and related purpose.

Sensitive information
Sensitive information is information or an opinion about an individual's:

- racial or ethnic origin;
- political opinion;
- membership of a political association or religious beliefs, affiliations or philosophical beliefs;
- membership of a professional or trade association or membership of a trade union;
- sexual preferences or practices; or
- criminal record,

that is also personal information or health information about an individual. (See Principles 2.1(c), and 10.)

Serious and imminent threat
A number of the Principles provide for circumstances where we might need to consider whether there is a "serious and imminent" threat to an individual's life, health or safety. For there to be a serious and imminent threat to an individual's life, health or safety:

- the threat must be to an individual's life or health; and
- there must be threat of bodily injury, threat to mental health, illness or death.

Imminent means that the threatened harm must be about to happen.

The threat must be serious, for example, murder or assault or threat of spreading an infectious disease. A specific threat of physical harm to a particular person in the Department or funded service provider usually counts as a serious threat. Threats to finances or reputation are not threats to life or health. Abuse, without a threat, directed to staff in general does not usually count as a serious threat (see Principles 1.5, 2, 6.1(a), and 10.1(c)).

Serious threat to public health or public safety
Various Public Health Acts while not necessarily defining public health give some indication of the range of conditions and threats that have been considered to be significant enough to warrant legislating about them in the interest of pubic health. Examples of conditions mentioned in public health acts are management of:

- sexually transmitted disease;
- diseases caused by environmental hazards and toxins;
- infection arising from an outbreak of infectious disease; and
- vaccine preventable diseases (see Principles 1.5, 2, and 6).

Use
Use of personal information relates to the handling of the personal information within the Department or funded service provider. Examples of uses of information are:

- adding information to a data base;
- forming an opinion based on information collected and noting it on a file.

APPENDIX B

PRINCIPLES OF FAIR INFORMATION HANDLING PRACTICES FOR THE DEPARTMENT OF HEALTH

PRINCIPLE 1 - COLLECTION

1.1
We must not collect personal information unless the information is necessary for one or more of our functions or activities

1.2
We must only collect personal information by lawful and fair means and not in an unreasonably intrusive way.

1.3
At or before the time we collect personal information from the subject of the information (or, if that is not practicable, as soon as practicable thereafter), it must take reasonable steps to ensure that the subject of the information is aware of:

(a) the identity of the Department or funded service provider and how to contact it;
and
(b) the fact that he or she is able to gain access to the information;
and
(c) the purposes for which the information is collected;
and
(d) to whom (or the types of individuals or organisations to which) it usually discloses information of that kind;
and
(e) any law that requires the particular information to be collected;
and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4
If it is reasonable and practicable to do so, we must collect personal information about an individual, only from that individual.

1.5
Where we collect personal information from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed under Principle 1.3 above, except to the extent that making the individual aware of the matter would pose a serious threat to the life or health of any individual.

PRINCIPLE 2 – USE AND DISCLOSURE

2.1

We must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) Both of the following apply:

(i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

and

(ii) The individual would reasonably expect us to use or disclose the information for the secondary purpose*;*

or

(b) The individual has consented to the use or disclosure;

or

(c) If the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) It is impracticable for us to seek the individual's consent before that particular use;

and

(ii) We will not charge the individual for giving effect to a request by the individual to us not to receive direct marketing communications;

and

(iii) The individual has not made a request to us not to receive direct marketing communications;

and

(iv) We give the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications;

or

(d) If the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) It is impracticable for us to seek the individual's consent before the use or disclosure;

and

(ii) The use or disclosure is approved by Departmental or Divisional Research and Ethics Committees and the research is conducted in accordance with approved guidelines;

and

(iii) In the case of disclosure - we reasonably believe that the recipient of the health information will not disclose the health information, or personal information derived from the health information;

or

(e) We reasonably believe that the use or disclosure is necessary to lessen or prevent:

(i) A serious and imminent threat to an individual's life, health or safety;

or

(ii) A serious threat to public health or public safety;

or

(f) We have reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of our investigation of the matter or in reporting our concerns to relevant persons or authorities;

or

(g) The use or disclosure is required or authorised by or under law;

or

(h) We reasonably believe that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

  (i) The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
  (ii) The enforcement of laws relating to the confiscation of the proceeds of crime;
  (iii) The protection of the public revenue;
  (iv) The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; and
  (v) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: *It is not intended to deter us from lawfully co-operating with agencies performing law enforcement functions in the performance of our functions.*

Note 2: *Sub-clause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in sub-clause 2.1 requires us to disclose personal information; we are always entitled not to disclose personal information in the absence of a legal obligation to disclose it.*

Note 3: *We are also subject to the requirements of Principle 9 if we transfers personal information to a person in a foreign country.*

2.2

If we use or disclose personal information under paragraph 2.1(h), we must make a written note of the use or disclosure.

2.3

Sub-clause 2.1 operates in relation to personal information that parts of the Department or funded service provider that is a body corporate has collected from a related body corporate as if our primary purpose of collection of the information was the primary purpose for which the related body corporate collected the information.

2.4

Despite sub-clause 2.1, the Department of Health or funded service providers that provide a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) The individual:
  (i) Is physically or legally incapable of giving consent to the disclosure; or
  (ii) Physically cannot communicate consent to the disclosure;

and

(b) A natural person (the carer) providing the health service for the Department or funded service provider is satisfied that either:
  (i) The disclosure is necessary to provide appropriate care or treatment of the individual; or
  (ii) The disclosure is made for compassionate reasons;

and

(c) The disclosure is not contrary to any wish:
  (i) Expressed by the individual before the individual became unable to give or communicate consent; and
  (ii) Of which the carer is aware, or of which the carer could reasonably be expected to be aware;

and

(d) The disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5

For the purposes of sub-clause 2.4, a person is responsible for an individual if the person is:

(a) A parent of the individual;

or

(b) A child or sibling of the individual and at least 18 years old;

or

(c) A spouse or de facto spouse of the individual;

or

(d) A relative of the individual, at least 18 years old and a member of the individual's household;

or

(e) A guardian of the individual;

or

(f) Exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;

or

(g) A person who has an intimate personal relationship with the individual;

or

(h) A person nominated by the individual to be contacted in case of emergency;

or

(i) a person defined by traditional Aboriginal law.

2.6

In sub-clause 2.5:

- *child* of an individual includes an adopted child, a step-child and a foster-child, of the individual.
- *parent* of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.
- *relative* of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

- *sibling* of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

PRINCIPLE 3 – DATA QUALITY

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

PRINCIPLE 4 – DATA SECURITY

4.1
We must take reasonable steps to protect the personal information we hold from misuse and loss and from unauthorised access, modification or disclosure.

4.2
In accordance with the provisions of the State Records Act, 1997, we must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under Principle 2.

PRINCIPLE 5 - OPENNESS

5.1
We must set out in a document clearly expressed policies on our management of personal information and must make the document available to anyone who asks for it.

5.2
On request by a person, we must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

PRINCIPLE 6 – ACCESS AND CORRECTION

6.1
Where we have possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that we are required or authorised to refuse to provide the individual with access to that record under any law.

6.2
Where we have possession or control of a record that contains personal information, we must take such steps (if any), that are, in the circumstances, reasonable to amend a record that is not accurate, complete or up-to-date, except to the extent that we are required or authorised to refuse to amend a record under any law.

PRINCIPLE 7 – UNIQUE IDENTIFIERS

We must not adopt as our own identifier of an individual, an identifier of the individual that has been assigned by:

(a) The Department of Health or another funded service provider; or
(b) an agent of the Department or funded service provider acting its capacity as agent; or
(c) a contracted service provider for a Department of Health or funded service provider contract acting in its capacity as contracted service provider for that contract; or
(d) a Commonwealth Government agency, its agent, or its contracted service provider

Unless:

(a) The use or disclosure is necessary for us to fulfil our obligations; or
(b) The use or disclosure is permitted under Principle 2.1

PRINCIPLE 8 – ANONYMITY

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with us.

PRINCIPLE 9 – TRANSBORDER DATA FLOWS

We must not transfer personal information about an individual to someone (other than the Department or funded service provider or the individual) unless:

(a) We reasonably believe that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to Principles contained in this Code;

or

(b) The individual consents to the transfer;

or

(c) The transfer is necessary for the performance of a contract between the individual and the Department or funded service provider, or for the implementation of pre-contractual measures taken in response to the individual's request;

or

(d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Department or funded service provider and a third party;

or

(e) All of the following apply:
    (i) The transfer is for the benefit of the individual; *and*
    (ii) It is impracticable to obtain the consent of the individual to that transfer; *and*
    (iii) If it were practicable to obtain such consent, the individual would be likely to give it.

or

(f) We have taken reasonable steps to ensure that the information which we have transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Principles contained in this Code.

PRINCIPLE 10 – SENSITIVE INFORMATION

10.1

We must not collect sensitive information about an individual unless:

(a) The individual has consented;

or

(b) The collection is required or authorised by law;

or

(c) The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

  (i) Is physically or legally incapable of giving consent to the collection;

  or

  (ii) Physically cannot communicate consent to the collection;

or

(d) If the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

  (i) The information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

  (ii) At or before the time of collecting the information, we undertake to the individual whom the information concerns that we will not disclose the information without the individual's consent;

or

(e) The collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2

Despite subclause 10.1, we may collect health information about an individual if:

(a) The information is necessary to provide a health service to the individual;

and

(b) The information is collected:

  (i) As required or authorised by law (other than this Act);

  or

  (ii) In accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind us.

10.3

Despite Principle 10.1, we may collect health information about an individual if:

(a) The collection is necessary for any of the following purposes:

  (i) Research relevant to public health or public safety;

  (ii) The compilation or analysis of statistics relevant to public health or public safety;

(iii) The management, funding or monitoring of a health service;

and

(b) That purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;

and

(c) It is impracticable for us to seek the individual's consent to the collection;

and

(d) The information is collected:

(i) as required or authorised by law;

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind us; or

(ii) in accordance with Departmental or Divisional or hospital Research and Ethics Committee approval

10.4

If we collect health information about an individual in accordance with subclause 10.3, we must take reasonable steps to permanently de-identify the information before we disclose it.

10.5

In this clause *non-profit organisation* means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.