



CHARTERED SECRETARIES
AUSTRALIA

Leaders in governance

14 August 2007

The Hon Chris Pearce MP
Parliamentary Secretary to the Treasurer
Parliament House
CANBERRA ACT 2600

By email to: Roz.Waters@aph.gov.au

Dear Chris

Shareholder privacy and protection

Chartered Secretaries Australia (CSA) welcomes the opportunity to comment on the issue of shareholder privacy and protection.

We have been advocating for some time that urgent changes are required in relation to access to and use of the register of members of companies and its treatment in the *Corporations Act*. At present, the law does not provide acceptable privacy rights for shareholders in relation to public access to and use of their details on the register.

CSA represents the company secretaries of most of Australia's largest public and private companies, all of whom are involved in maintaining registers of members and considering requests to access and use those registers. Our members have had to deal with requests to access and use the register from a number of bodies and have had to respond to shareholders who have objected, we believe quite rightly, to the use of that information. We have drawn on our members' experience in the formulation of this letter.

CSA will be making reference to the issues outlined in this letter in its submission to the PJC Inquiry into Shareholder Engagement and Participation which is currently open for comment.

Yours sincerely

Tim Sheehy
CHIEF EXECUTIVE

Shareholder privacy and protection

There is privacy legislation, at both Commonwealth and State level, designed to protect Australian citizens from the infringement of their privacy rights, yet the law relating to access to and use of the register of members does not meet acceptable privacy standards. CSA believes the law requires reform to provide increased privacy and protection to shareholders in relation to accessing and using their details on the register of members.

CSA recommends providing increased privacy and protection to shareholders in relation to access to and use of their details on the register of members. This would bring the Corporations Act into line with privacy obligations in place for all other financial dealings undertaken by Australians.

To achieve acceptable privacy rights, CSA recommends that third parties (including other members) should only have access to or a right to obtain copies of personal information concerning a shareholder on the share register:

- with the consent of the shareholder
- where the person seeking access has lodged a bidder statement with ASIC in connection with a takeover of the company
- where ASIC or the courts directs that a person is given access to or a copy of the register. ASIC or the courts could then be asked to apply a proper purpose test similar to the one introduced recently in the United Kingdom.

Summary of benefits of reform

The compelling reasons to support reform include:

- **Shareholders should have more acceptable privacy rights**

Companies and registries should only use or disclose personal information on the share register for the purposes for which the information was provided, that is, administering the shareholders' shareholdings in the company. This obligation should be subject to the same or similar exceptions to Principle 2 of the National Privacy Principles set out in Schedule 3 to the Privacy Act. At present, shareholder consent is not required to access or use their details on a share register.

- **There is a stark contrast between the protection of investors' privacy in bank accounts and superannuation and their lack of privacy in shareholdings**

The Corporations Act is out-of-date in relation to privacy rights in operation for Australians, and not aligned with the obligations to protect privacy relating to other forms of financial information. Australians have a right to privacy in relation to their wealth holdings in bank accounts, yet retail shareholders cannot prevent public disclosure of their wealth holdings in shares. There are also strict privacy requirements protecting investors in relation to superannuation contributions, which also contrast starkly with shareholders' lack of privacy.

- **Retail shareholders are primarily disadvantaged by the current lack of privacy**

Shareholders whose shareholdings are held indirectly via a custodian company are protected from the general public accessing their particulars. Currently, those Australians with direct shareholdings, that is, retail shareholders, are disadvantaged, despite the government encouraging Australians to directly invest. Direct shareholders, with less complex structures in the management of their shareholdings, should have similar levels of privacy and protection to those whose shareholdings are held indirectly.

- **A mechanism already exists for public disclosure of a substantial shareholding that could influence the company**

The substantial shareholding provisions in the Corporations Act provide a mechanism to require any shareholder with more than five per cent of shares to publicly disclose their interest in the company. This information is commonly used for understanding the levels of control of any particular company and CSA supports its retention on public policy grounds. Improved privacy rights for shareholders would not counteract this mechanism.

- **Mechanisms already exist for members to access and use the register for a proper purpose**

Members already have protection embedded in the legislation to ensure they can ask the company for a copy of the register if they have called a meeting; give a company notice of a resolution they propose to move at a general meeting and distribute statements to all members on any matter that may be considered at a general meeting. Increased privacy for shareholders would not affect existing rights to access and use the register for a proper purpose.

- **Mechanisms already exist regarding access to and use of the register as part of a takeover bid**

If offers are made to shareholders as part of a takeover offer, they are subject to regulation as set out in Part 6 of the Act, which is designed to protect shareholders. At present, any other offers are subject neither to regulation, nor to shareholder consent to disclosure of their details for the purpose of receiving such offers.

General comments

The register of members has historically been a public register and indeed under s 173 of the Corporations Act 2001 the register is open to inspection by any member without charge and any other person on payment of such fee as may be prescribed. In addition, any person (whether or not a member) may require a copy of the register and, on payment of the prescribed fee, the company must provide the copy within seven days.

CSA fully supports the obligation on any shareholder with more than five per cent of shares (s 671B in Part 6C1) to publicly disclose their interest in the company. There are compelling public policy reasons why it is important for members and the general public to be able to understand the levels of control of any particular company. However, CSA cannot point to any public policy objective that is achieved by having all shareholders' details open for inspection on a public register and obtainable upon request.

CSA contends that making all shareholders' details publicly available is an anachronism in the 21st century, when shareholders are no longer, as they were at the time of the introduction of the concept of limited liability, a small group of gentlemen in need of each other's particulars in order to confirm the application of a new concept. Today, shareholders can amount to millions of geographically dispersed individuals participating in wealth acquisition. Modern technology makes the disclosure of shareholders' particulars vulnerable to predatory behaviour, in a way that is not possible with other forms of wealth holdings such as bank accounts and superannuation.

CSA notes that Australians understand their right to privacy, as embodied in legislation, and increasingly query why they have no right to privacy as investors. With the growth of the numbers of shareholders in Australia, the question of providing privacy and protection to them has become more urgent.

Existing mechanism for protecting shareholders' rights

CSA notes that members already have protection embedded in the legislation to ensure they can:

- ask the company for a copy of the register (s 249E(3)) if they have called a meeting
- give a company notice of a resolution they propose to move at a general meeting (s 249N(1)). The company must ensure that all members receive notice of the resolution at the same time (s 249O(2)) and at the company's expense if the notice is received in time to send out with the notice of meeting (s 249N(3))
- distribute statements to all members on any matter that may be considered at a general meeting (s 249P(1)). The company must distribute it to all members (s 249P(6)) and at the company's expense if the statement is received in time to send out with the notice of meeting (s 249P(7)).

Such protections ensure that members can access the register for a proper purpose.

In relation to takeover bids, CSA notes that if a takeover offer has been made, it is subject to regulation as set out in Part 6 of the Act, which is designed to protect shareholders. At present, any other offers are subject neither to regulation, nor to shareholder consent to disclosure of their details for the purpose of receiving such offers.

Shareholders should have more acceptable privacy rights

Currently, shareholders have very limited privacy in respect of access to the register of members. Shareholders cannot prevent any member of the public from accessing their name, address and wealth holdings. Indeed, shareholders' lack of privacy in respect of public disclosure of their addresses and their financial affairs and their subsequent vulnerability to contact by people seeking to either make unsolicited offers to purchase their shares or sell services to them under the guise of supplying them with research is unprecedented.

There is privacy legislation, at both Commonwealth and state level, designed to protect Australian citizens from the infringement of their privacy rights, yet the law relating to access to the register of members falls short of other measures designed to protect citizens from invasions of privacy.

CSA notes that, with the recent introduction of the Do Not Call Register, Australians can choose not to receive telemarketing calls in their home, even if their name and address is available in a public telephone directory. Yet shareholders in Australia cannot choose *not* to receive either predatory offers to purchase their shares or offers of an investment and advisory group's latest research report on the company in which the shareholder invests, which automatically places the shareholder on the investment and advisory group's client list, despite the shareholder not having agreed to such an inclusion.

Such offers come from offerors who argue that their request for information from the register is relevant to the shareholding and therefore within the s 177(1A) exemption. CSA members are concerned that such offers may well be predatory or marketing, yet under the current law, cannot refuse access to the register, even if they believe such offers to be for an improper purpose. CSA members certainly know from their dealings with many disgruntled company shareholders, angry that their names and addresses have been provided to third parties, that such shareholders view these approaches as being for an improper purpose.

Companies and registries should only use or disclose personal information on the share register for the purposes for which the information was provided, that is, administering the shareholders' shareholdings in the company. This obligation should be subject to the same or similar exceptions to Principle 2 of the National Privacy Principles set out in Schedule 3 to the Privacy Act (see Appendix A).

Retail shareholders are the ones who are disadvantaged by the current lack of privacy. Shareholders whose shareholdings are held indirectly via a custodian company are protected from the general public accessing their particulars. Identifying these shareholders is feasible through the disclosure notice provisions in Part 6C.2 of the Corporations Act. However, this process of discovery is not the simple one of requesting a copy of a register of members, with full particulars.

As a result, those Australians with direct shareholdings, that is, retail shareholders, are disadvantaged, despite the government encouraging Australians to directly invest. Thus the current situation makes it acceptable for some shareholders to have more privacy than others by virtue of how they structure their affairs. CSA contends that direct shareholders, with less complex structures in the management of their shareholdings, should have similar levels of privacy and protection to those whose shareholdings are held indirectly.

The stark contrast between the privacy and protection offered to Australians in relation to their wealth holdings in bank accounts and superannuation, and the lack of acceptable privacy rights in relation to shareholdings requires legislative reform.

Recent legislation in the United Kingdom granting protection to shareholders

A proper purpose test has recently been introduced in the United Kingdom. The Companies Act UK provides that where a company receives a request for a copy of the register, it must either allow an inspection or provide a copy of the register or apply to the court. A company cannot simply decline a request. If the court is satisfied that the inspection, or copy, is not sought for a proper purpose, it directs the company not to comply with the request. It may also direct that the company does not have to comply with similar requests. If the court considers the request to be for a proper purpose, the company must immediately allow the inspection or supply the copy.

CSA recommendations for reform

CSA recommends providing increased privacy and protection to shareholders in relation to access to and use of their details on the register of members. This would bring the Corporations Act into line with privacy obligations in place for all other financial dealings undertaken by Australians.

To achieve acceptable privacy rights, CSA recommends that third parties (including other shareholders) should only have access to or a right to obtain copies of personal information concerning a shareholder on the share register:

- with the consent of the shareholder
- where the person seeking access has lodged a bidder statement with ASIC in connection with a takeover of the company
- where ASIC or the courts directs that a person is given access to or a copy of the register. ASIC or the courts could then be asked to apply a proper purpose test similar to the one in operation in the United Kingdom.

Appendix A

PRIVACY ACT 1988 - SCHEDULE 3

National Privacy Principles

Note: See section 6.

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

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

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

- (a) the identity of the organisation 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) the organisations (or the types of organisations) to which the organisation 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, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation 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;
 - (ii) the individual would reasonably expect the organisation 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 organisation to seek the individual's consent before that particular use; and
 - (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
 - (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she

- may express a wish not to receive any further direct marketing communications;
and
- (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; 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 organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure--the organisation 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 organisation 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
- (ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:
- (i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and
 - (iii) in the case of disclosure--the recipient of the genetic information is a genetic relative of the individual; or
- (f) the organisation 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 organisation 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;
 - (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 organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides 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 organisation 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 subclause 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.

2.6 In subclause 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.

3 Data quality

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

4 Data security

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

4.2 An organisation 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 National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation 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.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

- (a) in the case of personal information other than health information--providing access would pose a serious and imminent threat to the life or health of any individual; or
- (b) in the case of health information--providing access would pose a serious threat to the life or health of any individual; or
- (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- (d) the request for access is frivolous or vexatious; or
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- (g) providing access would be unlawful; or
- (h) denying access is required or authorised by or under law; or
 - (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (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; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 - by or on behalf of an enforcement body; or
- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:
 (a) must not be excessive; and
 (b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency; or
- (b) an agent of an agency acting in its capacity as agent; or
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
 (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
 (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

7.3 In this clause:

"identifier" includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an identifier .

8 Anonymity

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

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation 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 the National Privacy Principles; 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 organisation, 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 organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation 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 National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required 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;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation 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, an organisation 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 or under 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 the organisation.

10.3 Despite subclause 10.1, an organisation 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 organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required 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 the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation 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.