Mapping Privacy requirements onto the IT function

Part 2

Stephen Wilson

Privacy Law & Policy Reporter, Vol. 10 p32, June 2003

Mapping the NPPs onto business and technology management processes

The author has mapped the 10 National Privacy Principles, together with the sub-clauses from the Privacy Act, onto generic business and technology management processes of concern to most organisations.

The purpose of this mapping is to expose the breadth and depth of impact that Privacy compliance has on the IT function. It is hoped that such a mapping can lead to a common framework for analysing threats and risks to privacy compliance for each organisation. The subsequent detailed analysis can be varied in its detail according to the individual business context.

The mapping exercise could be readily modified or repeated for different sets of privacy principles, such as the Information Privacy Principles, or the health sector principles drafted so far by some state governments.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
NPP1: Collection	
1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.	– The organisation must document the types of personal information which are necessary to support its business, and ensure that its processes for collecting and maintaining that information are in line with the business requirements. – Existing collection points – especially forms and audit logs – must be reviewed and the nature of information evaluated. – Product/service development processes must include a review stage where new forms, audit log functions, and other collection methods are evaluated against the Collection Principle.
1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.	– The organisation should attempt to characterise its customers and others whose personal information is to be collected, so that rational decisions are made about the best means to gather that information. – Note the tension that can exist between minimising intrusion by taking information from other sources, and ensuring proper consent for that information to be taken.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
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.*	– A Privacy Statement or Policy (or a relevant subset of it) should generally be prominent or else readily available at every point where personal information is collected (such as web pages).
1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.	– The organisation should consider the possibility and practicality of authenticating individuals filling out forms by some means fit for purpose, to ensure that only the right individual is providing the information. – Note the possible tension between taking steps to authenticate the person filling out a form, and the desire to minimise intrusion and further data collection.
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 …	– The organisation should document the types of information it desires to collect from third parties, and have formal protocols in place to control that collection. – In particular, the third party providing information should have its own Privacy Policy and should have told its users of the possibility of information disclosure. The organisation must review the Privacy Policy and procedures of the third party before accepting any information from it.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
NPP 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 …* *(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; **or***	– All cases where an organisation anticipates disclosing personal data should be analysed and documented in advance of implementing information systems which handle such data. All "secondary purposes" should in particular be enumerated and reasons listed for using or disclosing information for those purposes. – The organisation should attempt to characterise the individuals about whom personal information is held, such that their 'reasonable expectations' about the handling of their information can be documented, and where necessary, tested.
*(b) the individual has consented to the use or disclosure; **or***	– Unambiguous consent must be captured via well designed consent forms, which inform the user where necessary the possibility of usage and/or disclosure which the user could not be reasonably expected to anticipate.
(c) if the information is not sensitive information and [the secondary purpose is direct marketing]: *(i) it is impracticable to seek the individual's consent before that particular use; and* *(ii) the organisation will not charge the individual for [opting out]; and* *(iii) the individual has not made a request to [opt out]; and* *(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention … that he or she may [opt out]; and* *(v) each written direct marketing communication … sets out the organisation's business address and telephone number and [electronic contact detail as applicable]; **or***	**For businesses involved with direct marketing:** – The organisation should characterise its users so it can confidently judge when it is truly impracticable to seek their consent for direct marketing activities. – Databases must be designed to record the status of each person's consent, and to ensure that if the consent status changes, that fact is promulgated in a timely and effective manner. – There should be a review mechanism in place so that every time a new communication is drafted, it is reviewed for compliance with paragraph 2.1(c)(iv).
(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 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*	**For organisations in the health sector:** – The organisation should characterise its users so it can confidently judge when it is truly impracticable to seek their consent for public health or safety activities. – The organisation must form a sound basis for its belief that the recipient will not disclose the information. Ideally, the recipient's Security Policy *and its actual practices* will be available for review by the organisation, or a reputable independent audit will have been undertaken and

National Privacy Principle and sub-clauses	**Impacts on business and technology**
information, or personal information derived from the health information; ***or***	the results made available.
(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***	– In many sectors it can be difficult to anticipate all realistic scenarios where life, health and safety depend on personal information being disclosed. The organisation should form its own view in advance about the possibility of such scenarios. – In general, organisations in healthcare, transport, mining, utilities, heavy manufacturing and so on could be expected to anticipate cases involving such threats to their users or the general public. – To manage unforeseen circumstances, the organisation should have a nominated Privacy Officer authorised to adjudge the reasonableness of ad hoc disclosures and document their deliberations.
(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***	– In many sectors it can be difficult for an organisation to anticipate all realistic scenarios where its customers or other users may be breaking the law. Few organisations would have the data or wherewithal to reliably detect unlawful activity. The organisation should form its own view in advance about the possibility of such scenarios. **For Banks:** – The risk management requirements of the Basel II agreement will require banks to pay more careful attention to possible unlawful activity by their customers. Since banks will be actively looking for such activity, and planning to make related disclosures, they should develop protocols that balance their obligations under Basel II and the Privacy Act.
(g) the use or disclosure is required or authorised by or under law; ***or***	– The organisation's nominated Privacy Officer should document all cases where information is required to be disclosed under law.
(h) the organisation reasonably believes that the use or disclosure is 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 [crimes] …;* *(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*	– The organisation's nominated Privacy Officer should document all cases where information is required to be disclosed under law.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
remedying of seriously improper conduct or prescribed conduct; *(v) the preparation for, or conduct of, proceedings before any court or tribunal …*	
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.	– See note against 2.1(h) above. – It is prudent for a written note to be made under other exceptional circumstances, as noted against 2.1(e) and (g) above.
2.3 [Explanatory clause relating to body corporates]	No notes.
2.4 [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***	**For organisations in the health sector:** – The database holding personal information that might be subject to this sub-clause should have fields to record the individual's capacity to give consent, as well as the fact of consent (as discussed against 2.1(c) above).
(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***	– Ideally the information system should limit access to the data sharing functions to authorised carers who are in a position to exercise the sort of clinical judgment implicit in this sub-clause. – If the information system software cannot control access to authorised carers, then manual procedures must be in place to document the decision of a carer to disclose information under this sub-clause.
(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***	– Note that the Electronic Transactions Act (1999) does not provide for wills and testaments to be signed electronically. It would therefore be prudent for e-health admissions and similar systems to still accommodate the recording of a living will in paper form with the patient's handwritten signature.
(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).	Reasonableness probably cannot be analysed satisfactorily in advance, given the complexity of healthcare. Instead, when disclosure under this sub-clause is documented (as noted against 2.4(b) above), the carer should also record their reasons for the extent of the disclosure.
NPP 3: Data quality	
An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete	– What is "reasonable" must be adjudged in the context of the organisation's business and sector. – The organisation should analyse and document its

National Privacy Principle and sub-clauses	**Impacts on business and technology**
and up-to-date.	business requirements for the accuracy and currency of personal information. – The organisation should characterise how it expects information to "age" over time. – The organisation should specify how it will make sure data quality is maintained, through mechanisms like periodic audit, consistency checks, update questionnaires, and so on. – Note the possible tension between the *completeness* of personal information called for by NPP 3 and the general minimisation of information collection required by NPP 1.
NPP 4: Data security	
4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.	– What is "reasonable" must be adjudged in the context of the organisation's business and sector. – The organisation must make a formal analysis of what security mechanisms (both technologies and practices) are appropriate in its business context, and in light of the actual risks associated with the specific information concerned. – Risks associated with privacy breaches should be explicitly covered in a Threat & Risk Assessment.
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 NPP 2.	– The organisation's Security Policy will typically include a section on data destruction. Such a section should additionally address the requirement to purge or de-identify personal information once it is no longer needed. – Where personal information has been archived, backed up or otherwise duplicated (but without leaving the custody of the organisation), then the efficacy of its destruction must be demonstrable. – Consideration should be given to the feasibility of selectively destroying an individual's data when that data is part of an audit log. – Where applicable, the organisation should adopt objective standards for de-identification of personal information. It should take account of sample sizes and provide some assurance as to the effectiveness of the de-identification. – To justify retaining information, the organisation should document its reasons in advance, in terms of its importance to the business.
NPP 5: Openness	
5.1 An organisation must … document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.	– This sub-clause would usually be addressed in the high level Privacy Policy or Statement.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
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.	– It is important that the organisation documents internally *precisely* what personal information it holds, for what purpose and so on; this coiuld be documented in the Privacy Management Strategy. A general description, as required by sub-clause 5.2, can be derived from this precise specification. – The organisation should consider what medium is reasonable for communicating the requirements of this sub-clause. While it is tempting these days to post privacy policy material on the web site, care must be taken in the event that some individuals tend to use media other than the Internet.
NPP 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, except to the extent that:	– The information system architecture must provide for definitive records of personal information to be provided when requested.
(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***	– Since it will be difficult in most sectors to anticipate scenarios where others may be personally injured as the result of providing an individual with access to their information, organisations should instead delegate general authority to a nominated Privacy Officer to make any necessary determinations under this sub-clause, and ensure that they document their reasons in each case where access is so denied.
(b) in the case of health information, providing access would pose a serious threat to the life or health of any individual; ***or***	– See note against paragraph (a) above.
(c) providing access would have an unreasonable impact upon the privacy of other individuals; ***or***	– Consideration should be given to database design which compartmentalises personal information held on different individuals, so that providing access to someone's information does not have to impact on the privacy of others.
(d) the request is frivolous or vexatious; ***or***	– Any judgment that a given request for access for frivolous or vexatious should be made by a nominate Privacy Officer and documented in each case where access is so denied.
(e) the information relates to … legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; ***or***	– Determination under paragraphs (e) through to (k) may have to be made by or with the assistance of the organisation's legal counsel.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
(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***	– See note against paragraph (e) above.
(g) providing access would be unlawful; ***or***	– See note against paragraph (e) above.
(h) denying access is required or authorised by or under law; ***or***	– See note against paragraph (e) above.
(i) providing access would be likely to prejudice an investigation of possible unlawful activity; ***or***	– See note against paragraph (e) above.
(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***	– See note against paragraph (e) above.
(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.	– See note against paragraph (e) above.
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 sub-clause 6.1 if it relies on sub-clause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where sub-clause 6.2 does not apply.*	– As part of its cataloging of all data collection methods, the organisation should analyse all instances of internally generated information, and note in advance where sensitive decision-making processes are likely to be connected to that data. This preparation will help the organisation when it comes to fielding requests for access. – Organisations in the Insurance and Finance sectors should take particular note of this sub-clause, as they commonly generate evaluative information on their customers.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
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.	– The reasonableness and feasibility of intermediaries should be considered in advance by the organisation, and a position documented in the Privacy Management Strategy and/or other relevant management documents.
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.*	– It would be prudent for a brief pricing analysis to be documented in advance, to make the case that its pricing is not excessive. – If the organisation does charge for access, then its Privacy Policy should anticipate the possibility of price increases, so that users are not taken by surprise.
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.	– The information system architecture must support proper promulgation of corrections. – What constitutes "reasonable steps" may depend on the nature of the information and its usual method of collection. – In most cases, where information is collected manually or directly from individuals, then its correction might best be handled by another form. – However, the most practicable means for correcting information collected in other ways may not be so obvious. When designing automatic collection systems and data generation systems, consideration should be given to the possibility of having to correct information.
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.	– Databases and other sub-systems where information is held should be designed in anticipation of the need to add annotations in the event of a disagreement over data quality. – It may be prudent to design the wording of such annotations in advance, if there is a relatively high chance that they will be called for.
6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.	– It is important that any foreseeable reasons for such denial be documented in advance, so that when such circumstances do arise, the organisation's response is not seen as ad hoc. – It may be prudent for the possible circumstances for denying access or correction to be described generally in the Privacy Policy.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
NPP 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 … or* *(c) a contracted service provider for a Commonwealth contract ….* *7.1A However, sub-clause 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).*	– Particular care is needed in relation to de facto identifiers in some sectors, like Medicare Numbers and other social security related identifiers. – This sub-clause does not appear to preclude the storing of identifiers assigned by agencies, nor even using those identifiers internally for indexing personal information records.
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 sub-clause 7.1, unless: *(a) the use or disclosure is necessary for the organisation to fulfill 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.*	– See note against paragraph 7.1 above.
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**.*	– See note against paragraph 7.1 above.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
NPP 8: Anonymity	
Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.	– It is currently rare in e-business for anonymous transactions to be practicable (principally because organisations usually have to authenticate their users to ensure they receive consideration for services it provides; there is as yet no electronic cash). – Having said that, it is wise not to dismiss the anonymity principle out of hand. The organisation should document the nature of its transactions and analyse the practicability of conducting any of them anonymously.
NPP 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 … 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 NPPs;* ***or***	– To form a 'reasonable belief' as to the legal environment of offshore recipients, the organisation should catalog in advance the locations of all anticipated recipients, and establish the status of privacy regulations in those places. – Where the status of a given jurisdiction is uncertain or changing, then the organisation should put in place a plan to follow up on it, and in the meantime, take care to forestall data flows into that jurisdiction.
(b) the individual consents to the transfer; ***or***	**For Banks*:*** – Under Basel II it is likely that banks will be required to disclose customer risk information with off-shore banks. Careful consideration must be given to customer education and consent processes in this new environment.
(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***	– In order to justify a transfer under this paragraph, the organisation should document in advance foreseeable cases where contractual arrangements are likely to require Transborder data flow.
(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***	– In order to justify a transfer under this paragraph, the organisation should document in advance foreseeable cases where contracts are entered into with third parties in the interests of the individual. – It would probably be prudent for the organisation to disclose the existence or possibility of such arrangements to the individuals concerned.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
(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***	– The organisation must carefully define the cases where this type of transfer is expected to occur, and document how it benefits the individual concerned. By characterising these cases, the organisation should be able to demonstrate where it is indeed impracticable to obtain consent, and where it is reasonable to presume that consent would be given.
(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 NPPs.	– In the absence of binding regulations in the location of off-shore recipients, the most "reasonable steps" are probably to (1) obtain the Privacy Policy of the recipient, (2) review that Policy against the NPPs, and (3) most importantly, obtain a reputable audit report or similar document that substantiates the recipient's compliance with their own policy.
NPP 10: Sensitive information	
10.1 An organisation must not collect sensitive information about an individual unless: *(a) the individual has consented;* ***or***	– Special care must be taken up-front to analyse and document the organisation's real business needs for collecting any *sensitive* information at all (recall that *sensitive* information relates to the individual's race, ethnicity, religion and so on, or to their health).
(b) the collection is required by law; ***or***	– When analysing their information collection requirements, the organisation should document any legal requirement to collect particular sensitive information, and cite the relevant Act or Regulation.
(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***	– See also notes at paragraph 2.1(e) above.
(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*	**For Not For Profit organisations:** – The organisation should determine if it will collect sensitive information on people who are not members but who have "regular contact" with it. If so, it should characterise in advance what constitutes "regular contact". – The organisation's membership process should be reviewed as necessary to ensure that proper consent to usage and disclosure of sensitive information is obtained from members as a matter

National Privacy Principle and sub-clauses	**Impacts on business and technology**
information without the individual's consent; ***or***	of course. – Information collection processes should be reviewed to see if sensitive information is inadvertently collected on individuals who are not members and so not have regular contact with the organisation. – The organisation should have a form review process in place to check collection methods whenever they change.
(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.	– In order to justify collection of sensitive information under this paragraph, the organisation should document in advance foreseeable cases where legal or equitable claims are likely to arise which require that particular information.
10.2 Despite sub-clause 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 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.*	**For organisations in the health sector:** – While it may be obvious to individuals in most cases dealing with health organisations that it is appropriate for health information to be collected, it would be prudent to document any particular legal requirements, and to cite any applicable rules laid down by competent bodies. – Organisations in allied health, paramedical, alternative medicine areas and so on, should carefully consider whether they are indeed delivering health services, and seek legal advice accordingly. **For Insurance companies:** – If the organisation is not providing a health service, but will collect health related information for legitimate purposes relating to health risks, then they should carefully note applicable laws which sanction such collection. – It may be prudent for insurance companies to cite the applicable laws when they seek consent to collect sensitive information.
10.3 Despite sub-clause 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 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***	– The organisation should make the case up-front, if it is not obvious, that it is engaged in public health and safety research.

National Privacy Principle and sub-clauses	**Impacts on business and technology**
(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***	– De-identification can become infeasible in cases where only a few individuals in a sample exhibit for instance a rare medical condition. Yet inclusion of records from such individuals can be necessary for public health and safety research. The organisation should expressly document such cases if they apply, to make its case under this paragraph. It may not be justified in retaining identifying data for some individuals if the conditions of those individuals is not the subject of the organisation's study.
(c) it is impracticable for the organisation to seek the individual's consent to the collection; and	– The organisation must describe up front its reasons for adjudging it to be impracticable to obtain consent.
(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.*	– The organisation should document any particular legal requirements, and cite any applicable rules laid down by competent bodies. – It may be prudent to draw peoples' attention to such laws and/or rules, at the time they sign up to a relationship with the organisation.
10.4 If an organisation collects health information about an individual in accordance with sub-clause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organization discloses it.	– The reasonableness of de-identification needs to be carefully determined according to the type of information and the statistical characteristics of the population from which it is collected. If an individual exhibits some rare trait, then that may to help identify them if information about that trait remains in their record. On the other hand, depending on the purpose, it may be necessary to retain information about such traits (see note at paragraph (b) above).
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.*	No notes.