Australian Government

Office of the Australian Information Commissioner

Revised Guide to information security

'Reasonable steps' to protect personal information

Consultation draft

August 2014

Contents

Background

The purpose of this guide

If the report is a particularly long one (eg in excess of 15 pages), consider including an Executive summary that provides a synopsis of the report and recommendations. Spell out any acronyms in full to enable this section to be read on its own. If not needed, delete this heading.

The Guide to information security (the guide) provides guidance on the reasonable steps entities are required to take under the Privacy Act 1988 (Cth) (Privacy Act) to protect the personal information they hold from misuse, interference, loss and from unauthorised access, modification or disclosure. This includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once the personal information is no longer needed, unless an exception applies.

The guide is intended for use by entities covered by the Privacy Act, including organisations, agencies, credit reporting bodies (CRBs), credit providers and tax file number recipients.[1]

This guide is aimed at helping entities meet their Privacy Act obligations by:

- outlining the circumstances that can affect the assessment of what steps are reasonable to take
- providing a non-exhaustive set of steps and strategies which may be reasonable for an entity to take.

This guide highlights the importance of preventative measures as part of an entity's approach to information security. Such measures can assist in minimising the security risks to personal information.

Although this guide is not binding, the OAIC will refer to this guide when assessing whether an entity has complied with its information security obligations in the Privacy Act.

The Privacy Act and the security of personal information

The Privacy Act includes a set of 13 Australian Privacy Principles (APPs) that regulate the handling of personal information by agencies and organisations. The APPs only apply to an 'APP entity', which is distinct from the broader term 'entity'. Both terms are used throughout this guide and are defined in the glossary section below.

APP 11 focuses particularly on information security matters; however each of the APPs is influenced by and influences security practices. An entity will need to be mindful of all of its obligations under the Privacy Act (along with other relevant legislative requirements) when considering the security of personal information. For example:

- APP 1.2 requires an entity to take reasonable steps to implement practices, procedures and systems to ensure the entity complies with the APPs, including APP 11
- under APP 8, if personal information is sent overseas to a contractor, an entity may need to consider the security infrastructure of the contractor
- the security measures employed by an entity must allow it, on request, to give an individual access to their personal information held by the entity, as required by APP 12; while at the same time prevent unauthorised access to that information.

APP 11

APP 11 requires APP entities (agencies and organisations) to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information.[2]

Specifically, APP 11.1 states that an APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs.[3] This requirement does not apply where the personal information is contained in a 'Commonwealth record' (defined in the 'Glossary' section below) or where the entity is required by law or a court/tribunal order to retain the personal information.

APP 11 applies to personal information that an agency or organisation holds. An entity holds personal information 'if the entity has possession or control of a record that contains the personal information'.[4]

The term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.

APP 11 is set out in full at Appendix B and the *Australian Privacy Principles guidelines* (APP guidelines) are available on the OAIC website. The APP guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.

Other Privacy Act obligations

Part IIIA of the Privacy Act and the registered CR (credit reporting) code made under s 26N of the Privacy Act contain security obligations (based on the requirements set out in APP 11) for CRAs and credit providers in relation to credit information files and credit reports.[5]

Relevant security provisions from Part IIIA are set out at Appendix B.

Also, Guideline 6.1(a) of the *Tax File Number Guidelines 2011* (TFN Guidelines), issued under s 17 of the Privacy Act, requires TFN recipients to take reasonable steps to protect TFN information.

TFN Guideline 6 is set out at Appendix B.

Links to additional information about the handling (including security) of credit information and TFNs can be found at Appendix C — 'Additional information security resources'.

Other legislation

There are also specific laws other than the Privacy Act which contain information security provisions that if breached are taken to be, for the purposes of the Privacy Act, an interference with the privacy of an individual.

The *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act) limits when and how health information included in an eHealth record can be collected, used and disclosed.[6] Unauthorised collection, use or disclosure of eHealth record information is both a contravention of the PCEHR Act and an interference with privacy for the purposes of the Privacy Act.[7]

Section 27 of the *Healthcare Identifiers Act 2010* (Cth) (HI Act) contains security obligations (similar to the requirements set out in APP 11) for entities who handle healthcare identifiers. A breach of s 27 of the HI Act will be taken to be, for the purposes of the Privacy Act, an interference with the privacy of the individual.[8]

OAIC's role

When the OAIC investigates a possible breach of an entity's information security obligations following a privacy complaint or when it conducts a Commissioner initiated investigation (CII) into an act or practice, including when information security has been breached, it considers two factors:

- the steps that the entity took to protect the information
- whether those steps were reasonable in the circumstances.

A breach of an entity's information security obligations may, depending on the circumstances, result in the Australian Information Commissioner exercising his or her regulatory powers.

Information on when and how the OAIC might exercise its powers is available in the OAIC's *Privacy Regulatory Action Policy* and *Guide to the OAIC's Privacy Regulatory Action* <<hyperlinks to be added when documents are published>>.

Managing information security

What is personal information?

Personal information is defined in s 6 of the Privacy Act as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[9]

There are some obvious examples of personal information, such as a person's name and address. Personal information can also include medical records, bank account details, photos, videos, biometric information (such as a thumb print or an iris scan) and even information about what an individual likes, their opinions and where they work.

Another important category of personal information in the Privacy Act is sensitive information. Sensitive information is a subset of personal information and is defined in the glossary.

The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information. Generally, sensitive information can only be collected with the individual's consent and there are increased privacy protections for this type of information.

Threats to personal information

The threats to personal information, outlined in APP 11, which an entity's information security controls should seek to guard against include:

- misuse — where personal information is used for a purpose that is not permitted by the Privacy Act.[10] For example, where an entity conducts an unauthorised search of records for personal information
- interference with personal information — such as where an attack on a computer system occurs that does not necessarily modify the content of the information, but leads to the exposure of personal information
- loss — including accidental or inadvertent loss of either:
  - electronically stored personal information, for example by failing to keep adequate backups of information when a system failure occurs due to a natural disaster or
  - hard copy documents, computer equipment or portable storage devices containing personal information that are physically lost, such as by leaving it in a public place.[11]

  Loss may also occur as a result of theft following unauthorised access or modification of personal information

- unauthorised access — when personal information that an APP entity holds is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity (including contractors and service providers).[12] For example, an unauthorised third party gaining access to personal information following a hacking incident
- unauthorised modification — where personal information held by an entity is altered by someone who is not permitted to do so, or is altered in a way that is not permitted by the Privacy Act. For example as a result of hacking or other illegal access of databases by someone outside the entity
- unauthorised disclosure — where information is released from an entity's control but the release is not permitted by the Privacy Act.[13] This includes an unauthorised disclosure by an employee of the entity. For example, where personal information is mistakenly released to someone other than the intended recipient.

These types of incidents and circumstances can arise as a result of human activity or natural events such as natural disasters. Human error is regularly claimed as the cause of privacy incidents, however it usually only occurs where entities do not have a privacy culture, training and appropriate practices, procedures and systems.

Privacy incidents may occur more frequently as a greater amount of personal information is collected in the online environment and a greater reliance is placed on electronic and online records. This will mean that taking steps to protect against external threats will become critical to meeting the Privacy Act's requirements. At the same time, entities will also need to guard against internal threats such as unauthorised access or misuse of personal information by their staff (the trusted insider risk).

Privacy and your business

Good privacy practice is important for more than just ensuring compliance with the requirements of the Privacy Act. If an entity mishandles the personal information of its customers, it can cause a financial or reputational loss to the customer and a loss of trust and considerable harm to the entity's reputation. If personal information essential to an entity's activities is lost or altered, it can have a serious impact on the entity's capacity to perform those activities.

It is important for entities to integrate privacy into their risk management strategies. Robust internal information-handling practices, procedures and systems (see 'Internal practices, procedures and systems' section below), for example a data-breach response plan (see 'Data breach' section below), can assist an entity to embed good information handling practices and to respond effectively in the event that personal information is misused, interfered with, lost or accessed, used, modified or disclosed without authorisation.

Many of the steps and strategies in this guide will also assist entities to ensure good handling of its other confidential information, such as commercially sensitive information.

Privacy by design, privacy impact assessments and information security risk assessments

Privacy by design

Entities will be better placed to meet their privacy obligations under the Privacy Act if they embed privacy protections in the design of their information handling practices, processes, systems, products and initiatives. Building privacy into personal information handling practices from the start, rather than 'bolting it on' at a later stage, is known as 'privacy by design'. 'Personal information security should be embedded early, including by choosing the appropriate technology and by incorporating information security measures that are able to evolve to support the changing technology landscape over time.

Entities should design their information security measures with the aim to:

- prevent the misuse, interference, loss or inappropriate accessing, modification or disclosure of personal information
- detect privacy breaches promptly
- be ready to respond to potential privacy breaches in a timely and appropriate manner.

If entities have appropriate security measures in place before they begin to handle personal information (either for the first time or in a new way), they will be better placed to meet their Privacy Act obligations. For example, entities should consider the security of personal information before they purchase, build or update ICT systems.

PIAs and information security risk assessments

One way to achieve privacy by design is to conduct a Privacy Impact Assessment (PIA). A PIA is a written assessment of an activity or function that identifies the privacy impacts of a project and sets out recommendations for managing, minimising or eliminating those impacts. Generally, a PIA should:

- describe the personal information flows in a project
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

The OAIC encourages entities to undertake a PIA for any new projects that involve the handling of personal information or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope and the extent to which personal information will be collected, used or disclosed. A PIA, especially one conducted at the early stage of a project's development, can assist entities in identifying any information security risks and inform the reasonable steps that an entity needs to take to protect the personal information they hold.

Under s 33D of the Privacy Act, if an agency proposes to engage in an activity or function involving the handling of personal information and if the OAIC considers that the activity or function might have a significant impact on the privacy of individuals, the OAIC may direct the agency to give the OAIC, within a specified period, a PIA about the activity or function.

A detailed guide to conducting PIAs is available from the OAIC website.

To inform the analysis of personal information security in the PIA, entities may need to conduct an information security risk assessment (also known as a threat risk assessment) in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA in that it involves the identification and evaluation of security risks, including threats and vulnerabilities, to information (including personal information) handled by an entity. Once the risks have been identified, the assessment will then examine the adequacy of an entity's information security controls (virtual and physical) in mitigating the risks to information held by the entity (including personal information) and whether those risks should be further mitigated.

As with PIAs the OAIC encourages entities to undertake an information security risk assessment for any new projects that involve the handling of personal information or when a change is proposed to information handling practices. Information security risk assessments can be undertaken in the design stage of a project and at any other time as required.

The findings of a PIA and information security risk assessment would inform the development of the entity's risk management and information security policies, plans and procedures. These policies would specify all the information security measures that are to be established and maintained by the entity against the risks and threats to the personal information that the entity handles (see 'Information security and privacy policies' section below).

Related matters

The following matters should also be considered by entities as part of the 'privacy by design' process:

- entities should have a governing body, committee or designated individual/s who are responsible for defining information security measures and plans to implement those measures (see 'Governance' section below)
- resources to guide and support these activities include those listed in the 'Information security resources' section at Appendix C, including domestic and international standards regarding information security (also see 'Standards' section below)
- depending on the circumstances, reasonable steps to protect personal information may include the preparation and implementation of a data breach policy and response plan (that includes consideration of whether to notify affected individuals and the OAIC in the event of a data breach).

Regular monitoring and review

If an entity has built privacy into its processes, systems, products and initiatives at the design stage, this does not mean that its security responsibilities have finished. The regular change of an entity's processes, information, personnel, applications and infrastructure, as well as the changing technology and security risk landscape, means that the regular review and monitoring of information security controls is crucial. The steps and strategies outlined below need to be implemented and maintained against this changing backdrop. Therefore, the OAIC expects that entities will regularly monitor the operation and effectiveness of the steps and strategies they have taken to protect personal information.

Entities that handle personal information as part of their functions and activities should consider the steps and strategies outlined in the 'Managing the information life-cycle' section below, so that personal information is protected throughout the stages of its life-cycle. This includes:

- the initial collection of the personal information by the entity
- the handling of the personal information by the entity, for example how it is used, disclosed, accessed and stored
- the destruction or de-identification of the personal information.

The steps and strategies discussed in the 'Managing the information life-cycle' section include an entity regularly reviewing its information handling practices during the personal information's life-cycle.

Information security resources

This guide does not seek to replace or endorse any existing government or industry resources regarding information security. However, depending on the circumstances, compliance with these resources may be a relevant consideration.

Additional resources on or related to, information security are widely available and entities should ensure they are aware of any relevant government, industry or technology specific standards, guidance, frameworks or obligations and incorporate these into their information security practices.

All entities will also need to be aware of relevant legislation (other than the Privacy Act) that imposes obligations in relation to personal information security such as the HI Act.

A list of additional information security resources is at Appendix C.

Circumstances that affect assessment of reasonable steps

The reasonable steps entities should take to ensure the security of personal information will depend on the circumstances, including the following:

- the nature of the entity holding the personal information
- the amount and sensitivity of the personal information held
- the possible adverse consequences for an individual
- the information handling practices of the entity holding the information
- the practicability of implementing the security measure, including the time and cost involved
- whether a security measure is itself privacy invasive.

All the circumstances outlined above, with the exception of the last, will also influence the reasonable steps that an organisation should take to destroy or de-identify personal information.

These circumstances (along with relevant examples from recent OAIC investigations) are discussed further below. The examples of OAIC investigations provided below were undertaken before the commencement of the APPs on 12 March 2014 and therefore refer to the National Privacy Principles (NPPs), specifically NPP 4 (replaced by APP 11). Reports of investigations relating to acts or practices prior to 12 March 2014 use the term 'own motion investigation' instead of CII. However the following examples are still relevant in relation to the circumstances that will affect whether an entity has taken reasonable steps to protect personal information.

Nature of the entity

The size of the entity, resources and the business model on which the entity operates are relevant to determining the steps the entity should take to protect personal information it holds. For instance, if an entity operates through franchises or dealerships, or gives database and network access to contractors, the steps that are reasonable for it to take may differ from the steps that are reasonable for a centralised entity to take. Equally the reasonable steps of that entity's franchisees, dealerships and contractors are likely to differ from the entity.

On 10 January 2011, the OAIC opened an investigation into Vodafone Hutchison Australia following allegations that customer information had been compromised. Vodafone's business model uses licenced dealerships to sell its products and services. These dealerships were given remote access to Vodafone's databases of customer information via a store login ID. Customer identification information held on the database, such as the number and expiry date of passports, was visible to all Vodafone staff and dealership employees through the login shared across the store.

Appropriate authentication of users is an important network security measure and the use of store logins reduces the effectiveness of audit trails to assist in investigations and access control monitoring. The use of shared logins means that anomalies may not be detected and if they are, they may not be able to be effectively investigated as the actions are not linked to an individual authorised user. Limiting access to personal information is another important means of protecting it from inappropriate access, use or disclosure.

While Vodafone had a range of security safeguards in place to protect the personal information on its system at the time of the incident, the use of store logins and the wide availability of full identity information caused an inherent information security risk. For this reason, in the OAIC's view, Vodafone had not taken reasonable steps to protect the personal information it held at the time of the incident and therefore it did not meet its security obligations under the Privacy Act.

The full investigation report is available on the OAIC's website.

Amount and sensitivity of personal Information held

Generally, as either or both of the amount and sensitivity of personal information held by the entity increases, so too will the steps that it is reasonable for that entity to take to protect that information.

The community generally expects that their sensitive information will be given a higher level of protection than non-sensitive information. This expectation is reflected in the increased privacy protections which apply to the handling of sensitive information.

Although it is not defined as sensitive information in the Privacy Act, people often expect that their financial information will be given a high level of protection.

On 24 May 2013, the OAIC and the Australian Communications and Media Authority (ACMA) investigated Telstra Corporation Limited (Telstra) following media allegations that personal information of Telstra customers was accessible online, which Telstra confirmed.

The OAIC's investigation focused on whether Telstra took reasonable steps to protect customer information from misuse, loss, unauthorised access, modification or disclosure.

Spread sheet files containing personal information about Telstra customers were hosted on a software platform by a third party service provider on behalf of Telstra. The OAIC received information that these files were publicly accessible online. This resulted in the personal information of approximately 15,775 Telstra customers being compromised, including full names, addresses and phone numbers. This included 1,257 customer accounts with active silent line services. Through its internal investigation, Telstra identified that there had been at least 166 unique downloads of the source files.

In assessing whether Telstra took reasonable steps to protect personal information, the OAIC considered what steps would have been reasonable in the circumstances to protect the personal information held. This included considering (amongst other issues) the nature of the personal information.

The OAIC noted that a breach of this type of personal information for the 1,257 Telstra customers with silent line services was not low risk. Further, the OAIC noted that varying risk levels may require an entity to take varying security precautions in order to meet the security requirements of the Privacy Act. The OAIC stated that it was a reasonable step for Telstra to implement security processes and procedures to address the heightened risk environment. For this (and other reasons), the OAIC and the ACMA found Telstra breached privacy laws in their respective investigations.

The OAIC's full investigation report is available on the OAIC's website.

Adverse consequences for an individual

When entities are assessing the steps that they take to protect personal information in their possession, they should consider the possible adverse consequences for the individuals concerned if the information is not secured.

For example, the mishandling of some kinds of sensitive information, such as health information which identifies an individual's medical condition:

- may provide the basis for discrimination or other forms of harm, and
- mishandling of this information may lead to humiliation or embarrassment, or undermine an individual's dignity.

Individuals may suffer adverse consequences such as reputational harm if sensitive information becomes public, or material harm if the information exposed enables identity theft or fraud. The likelihood of this harm occurring will influence whether it is reasonable to take a particular step.

On 20 July 2011, the OAIC opened an investigation into Medvet Laboratories, following reports that customer information held by Medvet had been compromised. Medvet offers services such as parentage and illicit drug testing and has an online store, which entails handling customers' sensitive health information as well as credit card details.

Medvet was notified that certain client information from orders placed via Medvet's online web store could be accessed via a Google search. Medvet initially advised that up to 692 online orders had been made accessible and captured via a Google cache. The orders were primarily for parentage or illicit drug testing services or products. However, a subsequent independent investigation into the incident stated that 848 online orders were stored in Medvet's online Webstore. The investigation also showed that 29 of these orders had been accessed over a two month period. Medvet advised that no customer names, client bank account details or details of any test results were disclosed.

The independent investigation revealed that the online ordering software used by Medvet did not include appropriate security and the development and quality management practices associated with the Webstore application were deficient. The Commissioner considered whether Medvet had taken reasonable steps to protect the personal information that it held. In considering whether reasonable steps had been taken, the Commissioner considered Medvet's particular circumstances, including that the type of information it held included sensitive health information. The Commissioner concluded that Medvet did not have reasonable steps in place to protect the personal information it held at the time of the incident and therefore did not meet its obligations under NPP 4.1.

The full investigation report is available on the OAIC's website.

Information handling practices

When determining the appropriate steps to protect personal information, entities should consider the ways in which they handle personal information. This may include considering how personal information is collected, used and stored.

An entity should also consider whether it outsources any of its information handling. If an entity holds information (the definition of 'holds' is discussed in the APP guidelines, Chapter B: Key concepts) and outsources information handling to a third party it will need to consider how the third party handles and secures the information.[14] Relevant factors include whether those third parties are subject to the Privacy Act in their own right.

For organisations, if a third party is not subject to the Privacy Act and if an entity takes reasonable steps to ensure the third party meets the entity's Privacy Act obligations, this in turn is likely to be considered as the entity taking reasonable steps to protect personal information under APP 11. Reasonable steps may include:

- having terms in the contract to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements
- conducting inspections of the third party's facilities and processes.

For agencies, s 95B of the Privacy Act requires agencies to take contractual measures to ensure that a contractor does not do an act, or engage in a practice, that would breach an APP.[15]

Similarly, it may be reasonable for entities that store personal information remotely, such as with cloud computing services that may be located overseas, to take different steps from, or additional steps to, an entity that stores information in its own facilities.[16]

In October 2013, the OAIC published a report on its investigation of AAPT and Melbourne IT in response to media reports that a server holding AAPT customer personal information had been compromised by the hacker group Anonymous.

The OAIC's investigation focused on whether AAPT and Melbourne IT took reasonable steps to protect customer information from misuse and loss and from unauthorised access, modification or disclosure.

The AAPT information was held on a server managed by WebCentral Pty Ltd, a webhosting business unit of Melbourne IT. The server on which AAPT information was held was accessed by Anonymous between 17 and 19 July 2012, with unauthorised information transfers occurring from 20 July 2012 to 22 July 2012. Subsequently, AAPT information was published by Anonymous on the internet.

The OAIC took the view that AAPT held the information for the purposes of NPP 4.1 (which has now been replaced by APP 11.1), despite it being stored on Melbourne IT's server. This meant that AAPT had an obligation to comply with NPP 4.1 in relation to the information.

Information on the server managed by WebCentral was accessed by Anonymous via the 'Cold Fusion' application installed on the server.

The 2005 contract between AAPT and WebCentral contained some provisions requiring WebCentral to have security arrangements in place for information held on the server. However, the contract did not require that:

- the information on the server be appropriately assessed and classified to determine whether it included personal information and the sensitivity of that information
- existing or emerging security risks in connection with the Cold Fusion application be identified and addressed or
- vulnerability scanning and effective lifecycle management of the Cold Fusion application occur.

In considering these factors, the OAIC came to the view that AAPT failed to take its own steps to appropriately manage and protect the information and did not have adequate contractual measures in place to protect the personal information held on the compromised server. AAPT continued to use a seven year old version of Cold Fusion which was generally known to have vulnerabilities when newer versions were available.

During the investigation, AAPT confirmed that not all of the compromised information was in use at the time of the hacking incident. NPP 4.2 (which has now been replaced by APP 11.2) required organisations to take reasonable steps to destroy or permanently de-identify personal information that is not being used or disclosed for any purpose under NPP 2 (use and disclosure is now covered by APP 6). To comply with this obligation, an organisation must develop systems or procedures to identify information the organisation no longer needs and a process for how the

destruction or de-identification of the information will occur.

The OAIC uncovered a low level of awareness of data retention requirements amongst staff or business units within Melbourne IT, and AAPT and data retention policies were not being followed at the time of the incident.

The OAIC came to the view that AAPT had breached the Privacy Act by failing to take reasonable steps to secure the personal information it held. The OAIC also found that the compromised servers contained some old customer information and that AAPT had failed to comply with its obligation to destroy or permanently de-identify information no longer in use.

The full investigation report is available on the OAIC's website.

Practicability of implementation

The practicability of implementing a security measure, including the time and cost involved, will influence the reasonableness of taking that step.

However an entity is not excused from taking particular steps to protect information by reason only that it would be inconvenient, time-consuming or costly to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances. In deciding whether these costs make a step unreasonable, an entity should have regard to other circumstances such as the sensitivity of the personal information and the risk to an individual if that information is misused, interfered with, lost, or inappropriately accessed, modified, or disclosed.

In 2009, the OAIC investigated a private medical centre following reports that a number of medical documents, including patients' prescriptions and pathology results, were found scattered in a public park adjacent to the centre. The name of the centre was visible on some of the documents as were patients' names, addresses and phone numbers. The medical centre informed the OAIC that a lock on a medical waste bin, kept outside at the rear of the centre, had been tampered with and the contents of the bin thrown around an adjacent public park.

Having regard to the sensitivity of the information held by the medical centre, the OAIC and the centre devised a number of steps that the centre could take to ensure that information was kept securely:

- The medical centre sought council approval to have secure fencing installed around the premises to reduce the risk of break-ins and vandalism
- It moved the secure medical waste bin inside the secured premises so that it could not be tampered with
- The bin was fitted with a new secure lock to which the medical centre manager held the key.

The medical centre developed policies and procedures for the secure destruction of personal information and trained medical and administrative staff in the proper destruction of both medical waste and medical documents.

The medical centre instructed its staff that medical documentation was not to be left with general medical waste for collection.

The centre obtained a shredder so that medical documents that were no longer needed could be securely destroyed on-site.

The OAIC determined that, following the implementation of these measures, the medical centre met its security obligations under the Privacy Act and closed her investigation.

The case note for this matter is available on the OAIC website.

Privacy invasiveness

It may not be reasonable to implement a security measure if it is itself privacy invasive. For example, requiring users to supply extensive personal information to identify themselves prior to giving access to their records under APP 12 may result in the entity collecting personal information that it would not otherwise require.[17]

Entities will need to balance the actions required to prevent disclosure of personal information to someone other than the individual concerned with the right of individuals to access their own personal information.

Steps and strategies which may be reasonable to take

Appropriate security safeguards and measures for protecting personal information need to be fully considered in relation to all of the entity's acts and practices. This should include taking steps and implementing strategies to manage the following:

- Managing the information life-cycle
- governance
- ICT security
- access security
- data breaches
- physical security
- personnel security and training
- destruction and de-identification
- internal practices, procedures and systems
- standards

This section outlines examples of key steps and strategies an entity should take in order to protect personal information and satisfy the security obligations in the Privacy Act. Although it may not be necessary for all entities to take all the steps and strategies outlined below, the OAIC will refer to this guide when assessing an entity's compliance with its security obligations in the Privacy Act.

The steps and strategies vary in ease of implementation and the impact that they will have on users. What is reasonable in the circumstances may vary between entities. What is reasonable may also change over time, for example, as a result of technological change or if an entity becomes aware that security measures which previously protected information are no longer adequate or if the entity handles information in a new way.

Entities should consider undertaking a PIA and an information security risk assessment for new projects that involve the handling of personal information or when a change is proposed to information handling practices, in order to inform the steps and strategies they will take to secure personal information (see 'Privacy by design' above and 'Managing the information life cycle' below).

The steps and strategies outlined below are not intended to be exhaustive. Entities should also consult relevant standards and guidance on information security, including any which are particular to their sector or industry (see 'Standards' and 'Information security resources' below).

The OAIC expects that entities will regularly monitor the operation and effectiveness of the steps and strategies they have taken to protect personal information (see 'Regular monitoring and review' section below).

Entities should be fully aware of all the personal information they handle, where it is kept and the risks associated with that information. Entities could undertake robust information asset management by developing and maintaining a register which provides a high level description of all the personal information handled by the entity. This will ensure that the entity's information security measures are comprehensive.

For additional information on information asset management and effective information governance (see 'Governance' section below), it is recommended that Australian Government agencies consult the OAIC's *Open sector information: from principles to practice: Report on agency implementation of the Principles on open public sector information* (February 2013). Entities may also find this information useful as a model of best practice.

Managing the information life-cycle

Entities that handle personal information as part of their functions and activities should consider the following steps and strategies (which are also discussed in more detail throughout the 'Steps and strategies which may be reasonable to take' section below) to ensure that personal information is protected and appropriately handled during the stages of its life-cycle.

The personal information life-cycle involves:

- planning and explaining how personal information will be handled by embedding privacy protections in the design of the entity's information handling practices before any personal information is collected (see 'Privacy by design' section above)
- the initial collection of the personal information by the entity due to a new act, practice, change to an existing project or as part of business as usual
- how the personal information is handled by the entity, for example how it is accessed, used, disclosed, maintained (up to date, accurate and complete) and held (storage and security)
- destruction or de-identification of the personal information under APP 11.2 or where the entity has other legal obligations to retain, destroy or de-identify the information.

Additionally, the life-cycle includes the passing of personal information to a third party for storage, processing or destruction. Entities should consider what steps are required to ensure that the third party will protect that information.

New acts and practices and changes to existing projects

- Are PIAs and information security risk assessments (see 'Privacy by design' above) conducted for new acts or practices, or changes in existing acts or practices that involve the handling of personal information?
    - Are new acts or practices or changes to acts or practices assessed in the design stage to identify whether they raise any privacy issues?

- Are there privacy protections embedded in the design of the entity's information handling practices? Have these protections along with any mitigation strategies recommended by any PIA or information security risk assessment been implemented?
- Are those strategies reviewed after a period following implementation to assess whether they are effective?

Regular review of personal information handling practices

- Does the entity regularly monitor and review the operation and effectiveness of its information handling practices?
  - Are changes implemented as a result of regular monitoring and reviews? Does the entity review its personal information collection practices at appropriate intervals to ensure that it does not handle unnecessary personal information?
- How does the entity verify the identity of an individual prior to giving access to their personal information?
- How does the entity ensure that the personal information of other individuals is not improperly disclosed when providing this access?
- Has the entity considered whether the steps required prior to granting access to an individual's personal information are proportionate to the amount and sensitivity of the information concerned to ensure that these steps do not unduly impede the individual's right to access their personal information?
- What processes does the entity use to identify customers/clients prior to disclosing their personal information by phone or in person? What measures does the entity take to ensure that these verification processes do not infringe customer/client privacy?
- What processes does the entity use to ensure mail containing personal information is sent to the intended recipient?
- What measures does an entity have in place to protect personal information during a system upgrade?
- What measures does the entity take to prevent information loss?
  - Does the entity have an information contingency plan that incorporates system back-ups? How is the system backed up, and how often?
  - Does the entity have an information contingency plan that incorporates disaster recovery?
- Is processing, storage or other handling of personal information out-sourced to a third party?
- What measures has the entity taken to protect personal information when it is passed to a third party?
- What steps does the entity take to ensure that contractors and third parties that handle personal information on its behalf do not breach information security requirements?

- Do contracts place explicit obligations on contractors in relation to their handling of personal information? Are security requirements, such as storing and processing personal information, explicitly addressed?
- Is compliance with contractual provisions regarding the handling of personal information reviewed or audited?
- What procedures are in place for ensuring that all personal information is either returned to the entity or destroyed at the end of the contract?
- Do invitations to tender require applicants to outline how they will address information security?

Destruction or de-identification of personal information

- If an entity is an agency, does it have policies, procedures and resources in place to facilitate the destruction or alteration of Commonwealth records in accordance with s 24 of the *Archives Act 1983* (Cth) (Archives Act)?
- If an entity is an organisation, does it have policies, practices, procedures and resources in place to determine whether personal information that it holds needs to be retained under law or a court/tribunal order, destroyed or de-identified? (see 'Destruction or de-identification of personal information' below)

Governance

Entities should establish clear procedures and lines of authority for decisions regarding information security. Entities could have a governing body, committee or designated individual/s who are responsible for managing the entity's personal information to ensure its integrity, security and accessibility, including defining information security measures and plans to implement and maintain those measures.

All entities, especially those that manage large and complex projects involving the handling of personal information, should have effective governance processes in place to ensure information security is consistently maintained.

Governance arrangements should be in writing, for example in the entity's internal practices, procedures and systems to ensure that relevant staff are aware of these arrangements.

- What governance arrangements does the entity have in place to implement and maintain its information security and privacy measures?
- Do the governance arrangements promote awareness and compliance with the information security and privacy obligations that apply to the entity?
- Are there clear procedures and lines of authority for decisions related to personal information security?
  - Are there governance controls in place which are responsible for the overall operational oversight and strategic direction of the entities' information handling projects?

  - Are there distinct areas or persons within the entity who have responsibility for security and privacy issues? If there are several areas or teams responsible for security and privacy, are there governance arrangements in place to ensure that they work together so that there is a focal point for privacy advice and solutions?
  - Are regular meetings held at the senior management and working level to discuss security and privacy issues and incidents?
- Are there change management processes in place which involve consideration of changes from the personal information security and privacy perspectives?
- Are there contractual governance arrangements in place to ensure that contractors do not act or engage in a practice that would breach the entity's security obligations under the Privacy Act — for example are regular meetings held with the contractor to discuss security issues or are there reporting requirements for contractors?
- Do governance arrangements include risk management and business continuity plans? For example are there designated persons responsible for the assessment of information security risks and implementation of business continuity plans?
- Are there ICT governance protocols in place? For example are there persons responsible for the accreditation and approval of information security controls used by the entity to ensure that each control is effective and appropriate?

ICT security

Effective ICT security requires protecting both computer hardware (the physical devices that make up a computer system) as well as the data (including personal information) that the computer hardware holds from misuse, interference, loss, unauthorised access, modification and disclosure. However, ICT security measures should also ensure that the hardware and the information stored on it remain accessible and useful to legitimate users.

Entities are expected to consider ICT security measures and the protection of personal information as part of their decision to use, purchase, build or upgrade ICT systems rather than attempting to address privacy later, for example after a privacy breach has occurred.

It is also expected that entities regularly monitor the operation and effectiveness of their ICT security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of personal information. This includes regularly applying patches (see 'Software security' section below) for known flaws in a timely fashion or using up to date software when previous versions are known to be flawed.

There is an expectation that entities which provide online customer services or engage in electronic commerce, such as online retail businesses, will utilise ICT security measures to ensure that their website, along with smart phones, mobile device applications (apps)[18], terminals, kiosks and other environments that may be connected to a network are secure

and that they provide a safe environment for individuals to make payments or provide their banking and personal information.

ICT security measures help mitigate the risks of external attackers and the damage caused by malicious software (or malware), computer viruses and other harmful programs. These programs can be used to gain unauthorised access to computer systems in order to disrupt or disable their operation and steal any personal information stored on those systems.

APP 6 outlines when an APP entity may use or disclose personal information. 'Unauthorised access' by a third party is a separate concept from 'disclosure'. For example, an APP entity is not taken to have disclosed personal information under APP 6 where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, failure by the entity to take reasonable steps under APP 11 to prevent unauthorised access such as a cyber-attack or a theft, including where the third party then makes personal information available to others outside the entity, may be a breach of APP 11. The OAIC has previously found, after investigation, that entities were in breach of the Privacy Act by not taking reasonable steps to prevent a data breach involving a cyber-attack.[19]

ICT security measures can also guard against unauthorised use or disclosure of personal information stored on a computer system while the system is being legitimately used. Such accessibility issues and unauthorised use or disclosure can occur as a result of:

- human error (for example, the misplacing of hardware components and peripheral devices such as laptops and data storage devices, noting that encryption and password protection can mitigate this risk)
- hardware or software malfunctions
- power failure
- system failure caused by natural disasters such as earthquakes, floods, and extreme weather conditions.

Whitelisting and blacklisting

Whitelisting describes listing entities, content or applications that are allowed to run on a computer or network. This allows only designated applications to run on a device. This can prevent malware from running. Whitelisting may offer greater protection than blacklisting (blocking material that is known to be harmful) as it is not dependent on identifying the material to be blocked. However a drawback is that it can also block harmless content that is not on the list.

- Is whitelisting or blacklisting of applications employed?
- Is whitelisted filtering of email attachments employed? If whitelisted filtering of email attachments has not been employed, has blacklisted filtering of email attachments been used instead? If so, what steps are in place to ensure the blacklist remains relevant, up to date and complete?

- Is whitelisting of web domains and IP addresses employed? If whitelisted filtering of web domains and IP addresses has not been employed, has blacklisted filtering of web domains and IP addresses been used instead?

Software security

Workstation level security software is an important security measure. However, similar software can also be deployed on other network components (for example on servers and network gateways).

- Has security software been deployed across all network components?
- Are the latest versions of software and applications in use?

Patches are software that is used to correct a problem with a software program or a computer system. Patches can result in a number of extra functions and features that should be assessed for their privacy impacts before they are installed.

- What processes are in place to ensure that patches and security updates to applications and operating systems are installed as they become available?
- Is the operating system running the latest version with the latest updates, fixes or enhancements installed?
- Is the entity's security software up to date?

Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack. Disabling functions such as AutoPlay or remote desktop, if they are not required, can make it harder for malware to run or an attacker to gain access.

- Are operating system functions that are not required disabled?

There is a risk that content delivered through websites can be used to arbitrarily access system users' files or deliver malicious code. This risk can be reduced by ensuring that software applications and web browsers, including 'add-ons' or 'plug-ins' (software that adds specific functions to browsers) are up to date. Disabling unused applications may also assist in preventing unauthorised access to a computer system.

- Are applications and web browsers configured for maximum security?

Entities importing data to a system should ensure that the data is scanned before it is opened to ensure that it does not contain any malicious content.

- Are all email attachments received from an external source scanned before they are opened?
- Are computer files scanned and checked for abnormalities at workstation level?

Web applications are an increasingly common technology that is accessed over a network, such as the Internet. Through a web browser, web applications allow users to perform certain functions. Common web applications include web-based email, wikis, directly updating personal details on databases and many other functions.

- Does the entity have security measures in relation to web applications?

Encryption

Encryption is when information is converted into a form that cannot be easily understood by unauthorised individuals or entities. Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to easily recover the contents of encrypted information, the correct decryption key is required. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective.

- What encryption methods are used by the entity? Has the entity considered whether it should employ encryption of:
  - Portable devices?
  - Email communications?
  - Databases used to store personal information?
  - Communication between internal information systems?
  - Hard drives?
  - Information stored over a network, such as the Internet or an entity's internal network, which has servers at a remote location?
- Is sensitive information held by the entity encrypted?
- How are decryption keys managed by the entity?
- Does the entity use a securely encrypted webpage for individuals who carry out transactions with the entity's website, such as making payments which also involve individuals providing their banking information?

Network security

Filtering of web traffic provides an opportunity to prevent harmful content from reaching user systems.

- Is both incoming and outgoing web traffic filtered?
- Are downloaded files quarantined from the network until it is established that they are safe (opened in a segregated testing environment such as a sandbox)?

Intrusion detection systems, which for example may involve using software applications that monitor network or system activities for malicious activities, anomalous behaviour, or policy violations, can be an effective way of identifying and responding to known attack profiles. Entities will need to ensure that such strategies are configured correctly, kept current and supported by appropriate security policies and processes.

- Does the entity maintain an intrusion detection system and regularly analyse event logs?
- How does the entity monitor and detect unauthorised downloading, transferring or theft of bulk data, for example through the use of personal storage devices?

Spoofed email is email in which parts of the email header are altered so that it appears to have come from a different source. Spammers may use this technique to try to bypass filters and make it appear as though email comes from a legitimate source. Such emails may ask the recipient to provide their own or other individuals' personal information.

- Is spoofed email blocked?
- Does the entity employ email validation and authentication systems, for example the Sender Policy Framework and DomainKeys?

Firewalls are intended to prevent unauthorised network access. There are different types of firewalls and ways of setting them up which will affect the level of protection offered.

- What sorts of firewalls are employed and how are they configured?

Separating an entity's network into multiple functional segments makes it difficult for an intruder to propagate inside the network. Proper network segmentation assists in the creation and maintenance of network access control lists. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.

- Is the network segmented and segregated into security zones?
- Are different security measures applied to different security zones, depending on the type of information in that zone and the risks associated with it? Does the information with the highest risk have the highest level of protection applied? What steps have been taken to ensure that this information is not inadvertently taken outside of the secured environment?

Testing

Testing of ICT security systems and processes may take a number of forms. Penetration testing uses approaches such as scanning networks to discover security weaknesses. Testing may be conducted internally or contracted out.

- Is testing of security systems and processes undertaken?
    - How often is testing conducted?
    - Who is responsible for conducting testing?
    - How is test data handled?
    - Is actual personal information or dummy data used for testing? If actual personal information is used, have a PIA and information security risk assessment been undertaken to assess the personal information flows caused by the testing?[20] Do the entity's internal practices, procedures and systems reflect the use of personal information for testing?
    - If testing identifies weaknesses, how is this reported and addressed?
    - Are independent vulnerability tests (penetration tests) of the entities' systems regularly undertaken?

Backing up

Backing up involves copying and archiving computer information so it may be used to restore the original when it is lost.

- Are backups set up to run frequently?
- Is all essential information included in backups?
- Does the entity have a data retention policy which reflects APP 11.2?
    - Does the entity review its backups to check that personal information that is no longer needed is:
        - destroyed or de-identified; or
        - if contained in a Commonwealth record, handled in accordance with the Archives Act; or
        - required by law or a court/tribunal to be retained? (see 'Destruction or de-identification of personal information' section below)
    - How far back is data recoverable?
- Are backups stored remotely to protect from natural disasters?
- Are backups stored securely to protect against misuse, interference, loss, unauthorised access, modification or disclosure of personal information?

Communications security

Personal information can be vulnerable to being improperly accessed or disclosed when it is transmitted. For example, unauthorised access by an employee to personal information may occur if it is left on a fax machine or printer or discussed over the telephone in an open office. Unauthorised disclosure to a third party may occur if, for example an email containing personal information is mistakenly sent to someone other than the intended recipient.

- Are staff advised on how to mitigate against unauthorised access if they discuss customers' or clients' personal information over the telephone?
- Are there procedures governing the transmission of personal information via fax or email?
- Are there procedures governing the transmission of personal information to offsite work locations?
- Are there procedures governing the printing of documents containing personal information?
- Does the entity employ encryption when communicating sensitive personal information?

Access security

Access security and monitoring controls help entities to protect themselves against internal and external risks by ensuring that personal information is only accessed by authorised persons.

Where appropriate, entities should consider limiting internal access to personal information only to those staff that require access to enable the entity to carry out the functions and activities for which the information is held (ie provide access on a 'need to know' basis).

'Unauthorised access' is a separate concept from 'disclosure' (see 'ICT security' section above). An entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However the entity may breach its security obligations under the Privacy Act if it did not take reasonable steps to protect the personal information from unauthorised access.

An entity could also restrict access to personal information that is linked to a pseudonym to authorised personnel.[21]

Authentication, authorised access and non-public content

Authentication to a system occurs when the user provides one of three types of information — something one knows (passwords or passphrases), something one has (a security token) and something one is (biometric information). Multi-factor authentication requires at least two types of information.

Entities should ensure that personal or sensitive information not intended for public release (non-public content) is not accessible through a public website. If entities host non-public content on their web servers, they should restrict access to this information to authorised and authenticated users only. This ensures that non-public content will not be accessed by unauthorised third parties including search robots[22] such as GoogleBot.[23] In conjunction with authentication, entities should also disable directory browsing when configuring web servers.[24]

- Is multi-factor authentication employed in circumstances where users are about to perform actions that may pose a higher security risk such as remotely accessing a system or where they are accessing sensitive/restricted personal information?
- Has the entity considered restricting access to personal information that is linked to a pseudonym to authorised and authenticated personnel?
- Has the entity considered restricting access to personal information to those staff necessary to enable the entity to carry out its functions and activities?
    - Is the number of users with administrative privileges limited to staff that require those privileges to carry out their functions and activities?
    - Is access revoked promptly when no longer required?
- Does the entity store non-public content on its webs servers?

- If so, is access to the personal information restricted to authorised and authenticated persons?
- Can the information be stored on a separate system which is not publicly accessible?
- Is directory browsing disabled on the entity's web servers?
- Are web servers configured to request search robots such as GoogleBot (via the robots.txt.file)[25] not to index, archive or cache files containing personal information?
- Does the entity regularly review and monitor its web servers to ensure that:
  - files containing non-public content are not vulnerable to being accessed by unauthorised persons?
  - they are aware of unusual or anomalous traffic on their website? (see 'Logs, audit trails and monitoring access' section below).

Passwords and passphrases

Passwords are sequences of characters that are used to gain access to a file, application, or computer system. Passphrases are sequences of words or other text used to gain access. They are similar to passwords but are often longer and more complex, which is intended to increase their effectiveness as a security measure.

Password generation can involve following particular patterns. There is a risk that a password protecting personal information which follows a particular pattern may be inferred by a person who is not authorised to access the information. Longer password patterns with many variations (in terms of both types of letters, numbers and characters used and their order) which are selected randomly rather than following a recognisable or known pattern are less likely to be guessed by unauthorised persons.

- Are strong passwords or passphrases enforced?
  - Are there mechanisms for changing them regularly?
  - Is reuse of passwords or passphrases blocked?
  - Is there a minimum length requirement?
  - Are staff (including contractors and service providers) trained in the importance of strong passwords or passphrases and how to choose them?
  - Is password complexity enforced? For example uppercase, lowercase, special character, numeric?
  - Are passwords generated by patterns which are randomly selected and complex in terms of their length, character and order?
  - Is sharing of passwords or passphrases permitted?
  - Are passwords or passphrases stored securely, such as in a 'hashed' or 'encrypted' format?
- Do accounts lock the user out after a specified number of failed logins?

  - Is a system administrator required to unlock accounts?
  - Are accounts that are unused or inactive for a period of time suspended?
  - How quickly are accounts removed or suspended once someone leaves the entity?
- Are screen lock programs activated when computers are not in use? Do the screensavers properly blank out computer screens or fill them with moving images or patterns so that no personal information can be displayed when computers are not in use?
  - Do computers automatically lock if left inactive or unattended for periods of time?
  - Are users advised to lock their computers when they leave their desks, even for short periods?

Collaboration

Entities that collaborate with external entities on specific projects which involve the use or disclosure of personal information in accordance with APP 6 should have effective controls in place to ensure that the personal information is only accessed by authorised persons within those other entities.

- Is personal information shared with (ie disclosed to) other entities (in accordance with APP 6)? If so, how is this managed to ensure that personal information is only accessed by authorised persons from the other entity or entities? How is access monitored?
  - Is the personal information disclosed to other entities using a secure method?
  - Is a platform that is managed, controlled or owned by another entity such as a contract service provider, used to share the information? If so, what controls are in place to limit access to the personal information to authorised persons only?
  - Is the information encrypted and password protected?
  - Is there an access control policy in place which applies to all entities handling the personal information?
  - Are there policies and controls in place to prevent the unauthorised downloading, transferring or theft of bulk data shared with other entities, for example through the use of personal storage devices?

Logs, audit trails and monitoring access

Unauthorised access of personal information can be detected by logs and audit trails. Ordering records chronologically is often the best for reviewing activity on a computer system to detect and investigate security and privacy incidents.

Access monitoring software which provides real time or close to real time dynamic review of access activity could also be used by entities to detect unauthorised access to personal information.

- What means exist to identify inappropriate access of files or databases which contain personal information, for example logs and audit trails? Is access by internal and external persons monitored? Are these measures mainly reactive (review of logs, responding to incidents) or do they also involve real time or close to real time monitoring of access activity? (also see 'Network security' section above)
- What points of access (such as access to devices, files, networks, databases, and websites) are audited by the entity? Are logs and audit trails implemented in a way that ensures their veracity and reliability? Are logs and audit trails monitored and retained on an on-going basis?
    - Does the audit trail indicate when an individual has accessed or viewed material, as well as when an individual has changed material?
    - Does the audit trail enable actions to be linked to individuals?
    - How often are checks/audits undertaken?
    - What procedures exist to address any issues, such as anomalous patterns of access, identified during audit?
    - How long are the audit logs kept for? Are they part of a backup process?

Individuals accessing and correcting their own personal information

Under the Privacy Act, entities must, on request, give individuals access to the personal information held about them unless an exception applies.[26] Individuals are also able to request correction of the personal information held about them.[27]

- What processes does the entity have in place to assess requests from individuals to access or correct their personal information?
    - How does the entity identify customers/clients prior to disclosing their personal information online, by phone or in person?
- What measures does the entity take to ensure that these authentication processes do not infringe customer/client privacy?
    - Are staff trained on how to prevent inadvertent disclosures, for example by avoiding leading questions during identity authentication checks?

Data breaches

In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist entities to contain the breach and manage their responses. Ensuring that staff (including contractors and service providers) are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective. The OAIC has published *Data breach notification: a guide to handling personal information security breaches*, which is available from its website.

- Is there a data breach response plan and does it flow logically from any broader information security plan?
    - Does the plan include a strategy to assess and contain breaches?

  - Does the plan clearly identify those actions that are legislative or contractual requirements?
  - Are staff educated about the plan and how to respond to data breaches?
  - Does the plan enable staff to identify data breaches and require that breaches be reported?
  - Does the plan establish clear lines of command and indicate responsible officers?
  - Does the plan outline clearly when affected individuals should be notified of breaches?
  - Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?
- Is the entity required to notify affected individuals and the OAIC under law?[28]

Physical security

Physical security is an important part of ensuring that personal information is not inappropriately accessed. Entities are to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, they should consider whether the workspace itself is designed to facilitate good privacy practices.

- What measures are used to control access to the workplace?
  - Are security and alarm systems used to control entry to the workplace?
  - Is it possible to identify staff movements from access logs?
- Have privacy and security been considered when designing the workspace?
  - Are workstations positioned so that computer screens cannot be easily read by third parties?
- Do visitors have access to general workspaces or are there designated areas for them?
- Are employees working on sensitive matters able to do so in a private/secure space?
- Is there a clean desk policy where personal information is being handled?
  - Is it enforced?
  - How often is it monitored?
- Do employees have access to secure storage spaces near their workstations to secure documents temporarily?
- What provisions are made for securing physical files containing personal information?
  - How is the movement of physical files recorded?
  - Are storage and movement of files containing personal information audited or monitored?

- On what basis is access to physical files granted?
- If files are placed in lockable cabinets or similar, are these storage units kept locked? How is access to keys controlled?

Personnel security and training

Human error can cause data breaches and undermine otherwise robust security practices. It is therefore important that all staff members (including contractors and service providers) understand the importance of good information handling and security practices. Privacy training may help staff to avoid practices that would breach the entity's privacy obligations by ensuring that they understand their responsibilities.

- Where appropriate, do staff have appropriate security clearance?
- What training is provided to staff regarding physical, ICT and communications security?
  - When is training provided to new starters?
  - Is training also provided to short term staff and contractors?
  - Is refresher training provided to staff? Does this occur on a regular basis?
  - Are staff informed of the entity's internal practices, procedures and systems which relate to the handling of personal information?
  - How are staff informed of changes to these practices, procedures and systems? (see 'Internal practices, procedures and systems' section below)
- Does staff training cover information security and appropriate handling of personal information?
  - Does training emphasise to staff the importance of not accessing personal information or databases unnecessarily?
  - Does training make it clear to staff what would constitute misuse of personal information?
  - Does training cover identity authentication procedures? Does this training cover recognising and avoiding inadvertent disclosures when verifying an individual's identity?
  - Does training emphasise to staff the importance of authentication processes not infringing customer/client privacy?
- Does training address the need to avoid weak passphrases and passphrase reuse?
- Are staff trained not to reuse the same password across multiple systems, such as different website logins?
- Does training address matters covered in workplace privacy and security policies (see below) and familiarise staff with those policies?
- Are staff reminded on a regular basis of their obligations to handle personal information appropriately?

  - Are there signs in the workplace or alerts on computer systems?
  - Do computer logon screens outline staff privacy and security responsibilities?
- How do employee exit procedures ensure that physical and network access is cancelled and personal information in the employee's possession (for example in files) is returned?
  - When is physical and ICT access revoked?
- When a staff member moves to a different position within an entity, is their access to personal information reviewed to determine whether there is a business need for them to retain the same access in their new role?
- Are staff trained to report privacy issues to the area or persons within the entity who have responsibility for security and privacy issues?

'Social engineering' is a term used to describe manipulating individuals into revealing confidential information or performing actions such as granting access to systems. 'Phishing' typically involves sending an email that appears to come from a legitimate organisation and attempts to trick the recipient into supplying confidential information. 'Spear phishing' is a personalised attack utilising personally relevant information to attempt to appear legitimate to a particular user.

- Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and social engineering?

Destruction or de-identification of personal information

General position

Under APP 11.2, where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. Also organisations must take reasonable steps to destroy or de-identify all copies of that personal information, including copies that have been archived or are held as backups.

However, depending on whether the entity is an agency or an organisation and the type of personal information involved, entities may have specific obligations under law or a court/tribunal order, to retain and/or destroy or de-identify personal information.

Examples of these obligations include:

- agencies have specific retention obligations for personal information that forms part of a Commonwealth record (discussed below)
- under the TFN Guidelines, TFN recipients are required to take reasonable steps to securely destroy or permanently de-identify TFN information that is no longer required by law to be retained, or is no longer necessary for a purpose under taxation law, personal assistance law or superannuation law
- under Part IIIA, different retention periods apply to specific types of credit information held by CRBs, with the CRB required to destroy the credit information

or ensure the information is de-identified within one month after the retention period for the information ends.[29]

Personal information held by an agency or a contractor of an agency – Commonwealth records

The requirement to take reasonable steps to destroy or de-identify under APP 11.2 does not apply if personal information is contained in a Commonwealth record, even if the agency no longer needs the personal information for any purpose for which it may be used or disclosed under the APPs.

An agency will instead be required to comply with the provisions of the Archives Act in relation to those Commonwealth records. Specifically, a Commonwealth record can generally only be destroyed or altered in accordance with s 24 of the Archives Act.

The term 'Commonwealth record' as defined in s 3 of the Archives Act is likely to include all or most personal information collected or received by agencies. It may also include personal information held by contracted service providers. While almost all the personal information held by agencies will be in Commonwealth records, there might be situations in which agencies do need to destroy or de-identify personal information. This is for the agency to determine.

- Does an agency have policies, procedures and resources in place to facilitate the destruction or alteration of Commonwealth records in accordance with s 24 of the Archives Act?

Personal information held by an organisation

Where an organisation holds personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information – in some cases, one or the other may be more appropriate. This obligation applies even where the organisation does not physically possess the personal information, but has the right or power to deal with it.

- Does the organisation have policies, procedures and resources in place to determine whether personal information that it holds needs to be: retained under law or a court/tribunal order, destroyed or de-identified?
- Are staff informed of document destruction procedures?

Destroying personal information – irretrievable destruction

Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an organisation to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

- Has personal information contained in hard copy records which are disposed of through garbage or recycling collection, already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding?

- Is hardware containing personal information in electronic form properly 'sanitised' to completely remove the stored personal information?
- Is destruction of personal information done in-house or outsourced?
- If outsourced, what steps has the entity taken to ensure appropriate handling of the personal information?
- How is compliance with data destruction procedures monitored and enforced?
- For hardware that cannot be sanitised, are reasonable steps taken to destroy the personal information in another way, such as by irretrievably destroying it?
- On a third party's hardware, such as cloud storage, where the third party has been instructed by the organisation to irretrievably destroy the personal information, have reasonable steps been taken to verify that this has occurred?

Destroying personal information held in electronic form – putting beyond use

Where it is not possible for an organisation to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'. For example, this could include where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information, which the entity is required to retain.

Personal information is 'beyond use' if the organisation:

- is not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surrounds the personal information with appropriate technical and organisational security. This should include, at a minimum, access controls including logs and audit trails, and
- commits to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format.

- Where it is not possible to irretrievably destroy personal information held in electronic format has the organisation taken reasonable steps to put the information 'beyond use'?

De-identifying personal information

De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the organisation or a third party.

Personal information is de-identified under s 6 of the Privacy Act, 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

An organisation that intends to comply with APP 11.2 by taking reasonable steps to ensure that personal information is de-identified should consider whether de-identification is appropriate in the circumstances.

- Does the organisation have policies, practices and procedures in place to determine when it is appropriate to de-identify personal information?
    - How does the organisation manage and mitigate the risk of re-identification?
- Where the personal information is held on a third party's hardware, such as cloud storage, and the organisation has instructed the third party to de-identify the personal information, has the organisation taken steps to verify that this has occurred?

For more information on when and how to de-identify information and how to manage and mitigate the risk of re-identification, agencies should consult the *Information Policy Agency Resource 1 — De-identification of Data and Information*; businesses should see *Privacy Business Resource 4 — De-identification of data and Information*.

Internal practices, procedures and systems

Under APP 1.2, an APP entity is required to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code. Privacy and information security protections have the best chance of being effective if they are integrated into an entity's internal practices, procedures and systems. Entities should document the internal practices, procedures and systems which they use to protect personal information.[30] These documents should clearly outline the privacy and information security measures that are established and maintained by the entity against the risks and threats to personal information. These documents should be regularly monitored and reviewed to ensure that they are effective.

Internal practices, procedures and systems which relate to privacy and information security, may be addressed in a single document or in a number of separate documents. Additionally, entities should ensure that relevant staff are aware of and have access to these documents and are trained regarding their responsibilities (see 'Personnel security and training' section above).

- Does the entity have documented internal practices, procedures and systems relevant to the handling of personal information which address information security and privacy matters, such as the physical, ICT and access security and other appropriate personal information handling practices?
    - Did a PIA and an information security risk assessment inform the development of the entity's practices, procedures and systems?
    - Is the entity's practices, procedures and systems documentation easy to understand?
    - If there are several documents involved, is it clear how the documents relate to each other, for example their hierarchy or order of importance?

  - Do the documents use language and concepts that are consistent with the Privacy Act?
  - Do the documents refer to the entity's obligations under the Privacy Act and other laws to protect personal information? Do they clearly explain how these obligations underpin these policies?
  - Are all staff, including short-term staff and contractors, aware of and able to access these documents easily?
  - Do these documents reflect the entity's current acts or practices? Are mechanisms in place for ensuring that the documents are updated and reviewed? For example, are regular reviews scheduled? Do designated staff members have responsibility for maintaining the documents?
  - Are mechanisms in place to enable staff members to seek clarification of the documents or suggest updates?
  - Are staff reminded to refer to the documents and informed of updates as they occur?
  - How does the entity ensure that the documents are being observed, for example are there governance mechanisms in place (such as designated privacy officers and regular reporting to the entity's governance body) to ensure this occurs?
  - Do the documents require that regular security reviews or audits are conducted?
  - What steps does the entity take if it becomes evident that staff members are not observing elements of the documents?
- Is there a conflict of interest policy in place that instructs staff members on how to proceed if they handle personal information relating to a person known to them?
- Are there clear polices governing the use of portable/mobile devices, use of staff's own devices (known as bring your own device (BYOD)), and procedures for taking work home?
  - Are there minimum standards for security of portable devices (such as password protection, encryption)?
  - Are return address labels placed on portable devices in case of loss?
  - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices?
  - If it is necessary to take personal information off the entity's premises, what steps does the entity take to ensure the security of personal information that is removed?
  - Is confidential business information segregated from personal user information?
- Is there a policy that covers information security when staff members work offsite, such as from home, a secondary site office or a temporary office?

- Is there an offsite work agreement that addresses data security, including the storage and security of personal information?
- What standards of physical security are applied to those workspaces, for example, the appropriate storage of physical files?
- If employees are given remote access to work ICT systems, what measures are in place to secure this access?
- Who has overall responsibility for the security of personal information at those workspaces?

Standards

Standards Australia states that standards are documents that set out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform the way they are intended to. Standards may be general or specific to particular industries or sectors, (for example the *National eHealth Security and Access Framework* (NESAF)[31], which is relevant to the health sector), or practices, such as electronic funds transfers.

Entities should consider using relevant international and Australian standards on information security to inform their risk based assessments of threats and vulnerabilities. Specific examples include the AS/NZS ISO/IEC 27000 series of information security management systems standards and the AS/NZS ISO/IEC 31000 of risk management standards.[32]

The Australian Signals Directorate produces the *Australian Government Information Security Manual* and the *Protective Security Policy Framework*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government. They may also be used by other government agencies (including state and territory agencies) as well as the private sector as a model for better security practice.

Compliance with standards can be tested internally or certified by a third party. Adopting a standard is one way that entities can gain some confidence regarding their security practices and that they are taking reasonable steps to protect personal information. However, complying with a standard does not absolve the entity of taking further steps to protect its holdings of personal information.

- What standards, if any, does the entity comply with?
- Has the entity considered standards particular to their industry or sector?
- How does the entity determine which standards to adopt?
  - If the entity determines not to adopt a standard, are the reasons for this decision clearly documented?
- How does the entity ensure that the standards employed are the most current and appropriate?
- Is internal auditing undertaken to ensure compliance with the standard?

- Is external auditing/certification undertaken to ensure compliance with the standard?
- If auditing reveals areas of weakness or non-compliance, how is this reported and addressed?

Appendix A — Glossary

Unless otherwise stated, terms used in this Guide have the same meaning as in the Privacy Act. Some of these terms are explained in more detail in the APP guidelines.

Agency has the meaning set out in s 6(1) of the Privacy Act and includes, amongst other things, a Minister, an Australian Government Department and a Norfolk Island agency.

APP entity means an agency or organisation and has the meaning set out in s 6(1) of the Privacy Act.

APPs means the Australian Privacy Principles which are set out in Schedule 1 of the Privacy Act.

CII means Commissioner initiated investigation, made under s 40(2) of the Privacy Act, where the Commissioner may, on his or her own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1. Investigations relating to acts or practices prior to 12 March 2014 use the term 'own motion investigation'.

Commonwealth record is defined in s 6(1) of the Privacy Act to have the same meaning as in s 3 of the *Archives Act 1983* (Cth).

CRB means credit reporting body and has the meaning set out in s 6 of the Privacy Act.

Credit provider has the meaning set out in s 6(1) of the Privacy Act.

CR Code means the *Registered CR (credit reporting) code*, a mandatory code that binds credit providers and CRBs. The CR code supplements the provisions contained in Part IIIA of the Privacy Act and the *Privacy Regulation 2013*. A breach of the CR code is a breach of the Privacy Act.

Cth means Commonwealth.

Data breach means, for the purpose of this guide, when personal information held by an entity is lost or subjected to unauthorised access, use, interference, modification, disclosure, or other misuse.

Entity means an agency, organisation or other person covered by the Privacy Act, including those covered by the APPs, Part IIIA and the *Tax File Number Guidelines 2011*.

Holds has the same meaning set out in s 6(1) of the Privacy Act.

NPPs means the National Privacy Principles, which used to apply to organisations unless an exemption applied. The NPPs were replaced by the APPs on 12 March 2014.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act and, in general, includes all businesses and non-government organisations with an annual turnover of more than

$3 million, all health service providers regardless of turnover and a limited range of small businesses (see ss 6D and 6E of the Privacy Act).

Personal information has the meaning as set out in s 6(1) of the Privacy Act:

> Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

PIA means Privacy Impact Assessment.

Privacy Act means the *Privacy Act 1988* (Cth).

Privacy Amendment Act means the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

Sensitive information has the meaning as set out in s 6(1) of the Privacy Act:

> (a) information or an opinion about an individual's:
>
> (i) racial or ethnic origin; or
>
> (ii) political opinions; or
>
> (iii) membership of a political association; or
>
> (iv) religious beliefs or affiliations; or
>
> (v) philosophical beliefs; or
>
> (vi) membership of a professional or trade association; or
>
> (vii) membership of a trade union; or
>
> (viii) sexual orientation or practices; or
>
> (ix) criminal record;
>
> that is also personal information; or
>
> (b) health information about an individual; or
>
> (c) genetic information about an individual that is not otherwise health information; or
>
> (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
>
> (e) biometric templates.

TFN means a tax file number and has the meaning set out in Part VA of the *Income Tax Assessment Act 1936* (Cth).

TFN information means information that connects a TFN with the identity of a particular individual (for example, a database record that links a person's name and date of birth with the person's TFN).

Appendix B — Information security obligations in the Privacy Act

Privacy Principles

11 Australian Privacy Principle 11 — security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part IIIA — Credit Reporting

20Q Security of credit reporting information

(1) If a credit reporting body holds credit reporting information, the body must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

(2) Without limiting subsection (1), a credit reporting body must:

(a) enter into agreements with credit providers that require the providers to protect credit reporting information that is disclosed to them under this Division:

(i) from misuse, interference and loss; and

(ii) from unauthorised access, modification or disclosure; and

(b) ensure that regular audits are conducted by an independent person to determine whether those agreements are being complied with; and

(c) identify and deal with suspected breaches of those agreements.

21S Security of credit eligibility information

(1) If a credit provider holds credit eligibility information, the provider must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

(2) If:

(a) a credit provider holds credit eligibility information about an individual; and

(b) the provider no longer needs the information for any purpose for which the information may be used or disclosed by the provider under this Division; and

(c) the provider is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the provider must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Civil penalty: 1,000 penalty units.

(3) If a credit provider is an APP entity, Australian Privacy Principle 11 does not apply to the provider in relation to credit eligibility information.

Tax File Number Guidelines 2011

Guideline 6 — Storage, security and destruction of TFN information

6.1 *TFN recipients* must take reasonable steps to:

(a) protect *TFN information* from misuse and loss, and from unauthorised access, use, modification or disclosure, and

(b) ensure that access to records containing *TFN information* is restricted to individuals who need to handle that information for *taxation law*, *personal assistance law* or *superannuation law* purposes.

6.2 A *TFN recipient* must take reasonable steps to securely destroy or permanently de-identify *TFN information* where it is no longer:

(a) required by law to be retained, or

(b) necessary for a purpose under *taxation law*, *personal assistance law* or *superannuation law* (including the administration of such law).

Appendix C — Additional information security resources

OAIC resources

- The *Australian Privacy Principles guidelines*, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.
- *Data breach notification: A guide to handling personal information security breaches*, which outlines steps that entities should consider in preparing for and responding to information security breaches, including notifying affected individuals.
- *Guide to the OAIC's Privacy Regulatory Action* <<link to be added when document is published>>, which provides detailed practical guidance about how the OAIC exercises its privacy regulatory powers. This document sits beneath the *Privacy Regulatory Action – Policy* (see below) and the *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013*.
- *Information Policy Agency Resource 1 — De-identification of Data and Information*, which provides general advice about de-identification, to assist agencies in balancing those objectives in information management.
- *Mobile Privacy: A Better Practice Guide for Mobile APP Developers*, which helps mobile device application (app) developers embed better privacy practices in their products and services, and help developers that are operating in the Australian market to comply with Australian privacy law and best practice.
- OAIC's *Privacy Regulatory Action Policy* <<link to be added when document is published>>, which explains the OAIC's overall approach and priorities when using its privacy regulatory powers and making related public communications.
- *Open sector information: from principles to practice: Report on agency implementation of the Principles on open public sector information* (February 2013), which is aimed at Australian Government agencies but may also be applicable to other entities as a model for best information management practice.
- *Privacy Business Resource 4 — De-identification of data and Information*, which provides general advice about de-identification, to assist businesses and other organisations to protect privacy when using or sharing information assets containing personal information.
- *Privacy fact sheet 6 — The binding Tax File Number Guidelines 2011 and the protection of tax file number information* – which provides guidance related to the handling of TFNs, including the security obligations of TFN recipients.
- *Privacy Impact Assessment Guide* which provides assistance on how to conduct a PIA.

Other resources

In addition, the following information security resources may be relevant to entities:

- CERT Australia is Australia's official national computer emergency response team. CERT Australia is the single point of referral for cyber security incidents impacting upon Australian networks. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.
- *Control Objectives for Information and Related Technology* (COBIT), which is an international framework created by ISACA for information technology (IT) management and IT governance.
- International standards published by the International Standards Organisation and Australian standards published by Standards Australia (see 'Standards' section of this guide).
- *OECD Guidelines for the security of information systems and networks* is a framework of principles applicable to the security of information systems.

The following resources may also be particularly relevant to Australian Government agencies and entities more generally:

- The *Australian Government Information Security Manual*, which governs the security of government ICT systems.
- The *Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements*, establishes a whole-of-government approach to the way different categories of information are treated when considering offshore or outsourced ICT arrangements.
- The *Australian Government Protective Security Policy Framework* (PSPF), which aims to enhance a stronger security culture and provide a common approach to the implementation of protective security across government. The PSPF may also be used by other government agencies (including state and territory agencies) as well as the private sector as a model for better security practice.
- *Agency cyber security responsibilities when transacting online with the public* - which aims to assist agencies to understand and address their responsibility to minimise the risk of harm to the public when transacting online with the Australian Government.
- The *Top 35 Strategies to Mitigate Targeted Cyber Intrusions*, developed by the Department of Defence, is a useful guide for both Government agencies and the private sector that contains a list of strategies to mitigate targeted cyber intrusions.
- The *National e-Authentication Framework*, developed by the Australian Department of Finance, assists Australian Government agencies and state jurisdictions in authenticating the identity of another party to a desired level of assurance or confidence.

Endnotes

[1] For more information on the jurisdiction of the Privacy Act see www.oaic.gov.au.

[2] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 86.

[3] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.

[4] See s 6(1) of the Privacy Act.

[5] See ss 20Q and 21S of the Privacy Act and cl. 15 of the registered CR code. The provisions in Part IIIA make it clear whether the obligations in Part IIIA replace relevant APPs or apply in addition to relevant APPs. For example, s 21S states that if a credit provider is an APP entity, APP 11 does not apply to them in relation to credit eligibility information. Part IIIA also contains provisions regarding the destruction or de-identification of credit information files and credit reports in certain circumstances.

[6] See Part 4 of the PCEHR Act.

[7] See s 73 of the PCEHR Act.

[8] See s 29 of the HI Act.

[9] For more detail on the definition of 'personal information' see the APP guidelines, Chapter B: Key concepts.

[10] APP 6 sets out when an entity is permitted to use personal information. APPs 7 and 9 also contain requirements relating to an organisation's use of personal information for the purpose of direct marketing, and use of government related identifiers, respectively.

[11] Loss does not apply to intentional destruction or de-identification of that personal information that is done in accordance with the APPs.

[12] Under s 8(1) of the Privacy Act, an APP entity needs to take reasonable steps to ensure that an employee does not carry out an unauthorised disclosure of personal information 'in the performance of the duties of the person's employment'.

[13] Under s 8(1) of the Privacy Act, an APP entity needs to take reasonable steps to ensure that an employee does not gain unauthorised access to personal information 'in the performance of the duties of the person's employment'.

[14] In situations, where an entity outsources information handling to third parties, the entity only needs to comply with APP 11 where it 'holds' the personal information in an outsourcing arrangement. In other words, if the entity releases the information beyond its effective control, this is a disclosure – it will not continue to hold that piece of disclosed information, so it would not need to comply with APP 11. However for overseas disclosures, the entity might have continuing obligations through the accountability provisions in APP 8.

[15] In particular, the agency must ensure that the contract does not authorise a contractor to do or engage in such an act or practice. An agency must also ensure the contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.

[16] Where an APP entity engages a contractor located overseas to perform services on its behalf, it must consider whether the provision of personal information to that contractor is a disclosure or a use. If it is a disclosure, the entity will also need to comply with APP 8 which applies to the cross-border of personal information. If the provision of personal information to the contractor is a use (ie the entity does not release the subsequent handling of personal information from its effective control), the entity would not need to comply with APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in certain limited circumstances set out in the APP guidelines, Chapter 8, paragraph 8.14.

[17] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

[18] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services. The OAIC's *Mobile Privacy: A Better Practice Guide for Mobile APP Developers* is available on the OAIC website.

[19] Examples include the OAIC's investigations into First State Super Trustee Corporation and the AAPT and Melbourne IT, available on the OAIC website.

[20] An example of a 'use' that an individual may be taken to reasonably expect is use for the secondary purpose of a normal internal business practice, such as auditing, business planning, billing or de-identifying personal information. The OAIC will generally consider dummy testing of ICT security systems to be a normal internal business practice (subject to the exception in APP 6.2(a). For further information see APP guidelines, Chapter 6, paragraph 6.22.

[21] APP 2 covers issues related to anonymity and pseudonymity.

[22] Search robots or bots are software programs which run automated repetitive tasks over the Internet. They are most commonly used by web search engines and other sites for 'Web crawling' or 'Web spidering'. This involves a search engine using bots to discover new and updated pages which are then added to the search engine's index of Web content.

[23] GoogleBot is Google's web crawling bot.

[24] Directory browsing gives permission to users to view a listing of the files in a web server. If directory browsing is disabled, an 'Access Forbidden' error message is displayed if the user attempts to access either a file or folder on the web server.

[25] One way to prevent GoogleBot from crawling content on a website is to use robots.txt to block access to files and directories on a server. 'Robots.txt' is a protocol used to request cooperating search robots not to access all or part of a website which is otherwise publicly accessible. Search engines comply with 'robots.txt' voluntarily and the OAIC has noted that most search engines comply with 'robots.txt', including Google, Bing and Yahoo.

[26] See APP 12. Along with the right to request access under the Privacy Act, individuals have a right under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to information held by Australian Government agencies.

[27] See APP 13 - where an individual requests an APP entity to correct their personal information, APP 13.1 provides that the entity must take reasonable steps to correct the personal information it holds, to ensure it is accurate, up-to-date, complete, relevant, and not misleading, having regard to the purpose for which it is held'. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

[28] Particular entities have mandatory data breach notification reporting obligations under s 75 of the PCEHR Act.

[29] See ss 20V and 20W of the Privacy Act.

[30] Documentation regarding an entity's internal practices, procedures and systems is distinct from an entity's external facing APP privacy policy required under APP 1.3 which outlines the entity's management of personal information. An APP privacy policy must also contain certain information set out in APP 1.4. Other information that could be included in the APP privacy policy includes information about retention or destruction practices or obligations that are specific to the entity. For further information see the APP guidelines, Chapter 1.

[31] The NESAF is a comprehensive suite of documents regarding health security for the health industry and specific Australian health organisations. The NESAF aims to assist health organisations in meeting their security obligations. The NESAF is available at: < www.nehta.gov.au/our-work/security>.

[32] Further information regarding Australian and international standards is available from the Standards Australia website at <www.standards.org.au> and the International Organization for Standardization website at: <www.iso.org>.