Australian Government

Office of the Australian Information Commissioner

Guide to information security

April 2013

'Reasonable steps' to protect personal information

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the OAIC.

ISBN 978-1-877079-98-6

Creative Commons

This publication should be attributed as: Office of the Australian Information Commissioner, *Guide to information security: 'reasonable steps' to protect personal information* (2013).

Enquiries regarding the licence and any use of this report are welcome.

Office of the Australian Information Commissioner
GPO Box 2999
CANBERRA ACT 2601
Tel: 02 9284 9800
TTY: 1800 620 241 (no voice calls)
Email: enquiries@oaic.gov.au

Contents

Key messages

- This guide is intended for entities, including Australian, ACT and Norfolk Island Government agencies, and private sector organisations that are covered by the *Privacy Act 1988* (Cth). It is also relevant to credit reporting agencies, credit providers and tax file number recipients.
- This guide provides guidance on information security, specifically the reasonable steps entities are required to take under the Privacy Act to protect the personal information they hold.
- This guide discusses some of the circumstances that the Office of the Australian Information Commissioner takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure.
- This guide also presents a set of non-exhaustive steps and strategies that may be reasonable for an entity to take in order to secure personal information. Although it is not necessary for all entities to take all the steps and strategies outlined in this guide, the OAIC will refer to this guide when assessing an entity's compliance with its security obligations in the Privacy Act.
- What is reasonable may vary between entities and may also change over time. Therefore it is important that entities regularly monitor and review the relevance and effectiveness of security measures which protect personal information.
- In some circumstances the use of electronic and online records can increase the possibility of personal information being misused, lost or inappropriately accessed, modified or disclosed. It is critical that entities consider the steps and strategies required to protect and secure personal information they hold in order to meet the Privacy Act's requirements.
- Entities should build privacy and information security measures into their processes, systems, products and initiatives at the design stage. This, and other preventative steps, assists entities to ensure that they have appropriate measures in place to minimise the security risks to personal information they hold.
- Entities should consider undertaking a Privacy Impact Assessment and an information security risk assessment for new acts or practices, or changes in existing acts or practices that involve the handling of personal information in order to identify the steps and strategies they will take to secure personal information.

Key terms

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

APPs means the Australian Privacy Principles which are set out in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Reform Act). The APPs will commence on 12 March 2014.

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

Credit provider has the meaning set out in s 6 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, modification, disclosure, or other misuse.

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

IPPs means the Information Privacy Principles set out in s 14 of the Privacy Act, which apply to agencies unless a listed exemption applies (see s 7 of the Privacy Act).

NPPs means the National Privacy Principles set out in Sch 3 of the Privacy Act, which apply to organisations unless a listed exemption applies (see s 7 of the Privacy Act).

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 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 of the Privacy Act:

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

PIA means Privacy Impact Assessment.

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

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

Sensitive information has the meaning as set out in s 6 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) sexual preferences 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.

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

Background

The purpose of this guide

This 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, loss and from unauthorised access, use, modification or disclosure.

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 examples 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.

Who is this guide for?

This guide is intended for entities, including Australian Government, ACT Government and Norfolk Island agencies, and private sector organisations that are covered by the Privacy Act. It is also relevant to credit reporting agencies (CRAs), credit providers and tax file number (TFN) recipients.

What is this guide about?

The Privacy Act regulates how entities handle individuals' personal information. Along with obligations regarding the collection, use, disclosure and the provision of access to personal information, the Privacy Act also requires entities to take 'reasonable steps' to protect the personal information that they hold from misuse, loss and from unauthorised access, use, modification or disclosure. These obligations to protect personal information are set out in Information Privacy Principle (IPP) 4 for agencies[1] and National Privacy Principle (NPP) 4 for organisations (see Appendix A for IPP 4 and NPP 4).[2]

Additionally, s 18G(b) of the Privacy Act imposes equivalent requirements on CRAs and credit providers in relation to credit information files and credit reports. 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 safeguard TFN information.

1 The IPPs are set out in s 14 of the Privacy Act and apply to Australian Government, ACT Government and Norfolk Island agencies.

2 The NPPs are set out in s 3 of the Privacy Act and apply to large businesses (with an annual turnover greater than $3 million), all health service providers and some small businesses and non-government organisations.

Each of the privacy principles (not just IPP/NPP 4) is impacted by security practices and 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, the security measures employed by an entity must allow individuals to access their personal information, as required by the Privacy Act, while at the same time prevent unauthorised access to that information.

When the Office of the Australian Information Commissioner (OAIC) investigates a possible breach of IPP/NPP 4, s 18G(b), or Guideline 6.1(a) of the TFN Guidelines, or conducts an own motion investigation 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.

This guide discusses some of the circumstances that the OAIC takes into account when assessing the reasonableness of steps. It will then present a range of steps and strategies that may be reasonable for an entity to take. However, these steps and strategies are not intended to be an exhaustive and complete set of measures for securing personal information. It is important that agencies and organisations regularly review the adequacy and relevance of security measures that they have in place to protect the personal information they handle.

Privacy law reform

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Reform Act) passed through the Australian Parliament on 29 November 2012 and received royal assent on 12 December 2012. The Reform Act introduces a number of changes to the Privacy Act. These changes include a single set of 13 new privacy principles for both the public and private sector, called the Australian Privacy Principles (APPs), which will replace the existing IPPs and the NPPs.

The security of personal information is dealt with in APP 11. The obligations in APP 11 are similar to those in NPP/IPP 4. However, APP 11 will require an entity to take reasonable steps to protect personal information from 'interference', as well as from misuse, loss, unauthorised access, modification or disclosure. The inclusion of 'interference' in APP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems).

The OAIC is developing guidelines to the APPs that will include guidance on APP 11. The APP guidelines will be made available prior to the commencement of the Reform Act on 12 March 2014.

The Reform Act also contains new credit reporting provisions, which include security obligations for CRAs (called 'credit reporting bodies' in the Reform Act) and credit providers based on the requirements set out in APP 11. The new credit reporting provisions also contain additional security obligations which apply to credit reporting bodies, and will be supplemented by a CR (credit reporting) code.

Managing information security

What is personal information?

Personal information is defined in s 6(1) of the Privacy Act as:

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

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. The Privacy Act defines sensitive information as:

(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) sexual preferences 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.

Under the Reform Act the definition of sensitive information in s 6(1) of the Privacy Act will be amended to include biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

The Privacy Act imposes stricter rules about when sensitive information can be collected and how it must be handled. Generally, sensitive information can only be collected with the individual's consent and there are tighter restrictions on how this type of information can be used and disclosed.

Risks to personal information

Entities have security obligations under the Privacy Act, including in IPP 4 and NPP 4, to take reasonable steps to keep personal information safe and secure from unauthorised access, modification or disclosure and also against misuse and loss.

There are a variety of ways in which personal information may be misused, lost or inappropriately accessed, modified or disclosed. Common situations that an entity's information security measures should seek to guard against include:

- unauthorised access or misuse of records by a staff member (including contractors and service providers)
- failure to store records containing personal information appropriately or dispose of them securely
- loss or theft of hard copy documents, computer equipment or portable storage devices containing personal information
- mistaken release of records to someone other than the intended recipient
- hacking or other illegal access of databases by someone outside the entity.

The possibility of these types of incidents occurring may be increased due to greater collection of personal information in the online environment and the reliance on electronic and online records. This will mean that taking steps to protect against external attacks will become critical to meeting the Privacy Act's requirements. At the same time, entities will also need to guard against internal risks such as unauthorised access or misuse of personal information.

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 clients or customers, it can cause a loss of trust and considerable harm to the entity's reputation. Additionally, if personal information that is essential to an entity's activities is lost or altered, it can have a serious impact on the entity's capacity to perform its functions or activities.

It is important for entities to integrate privacy into their risk management strategies. Robust information-handling policies, including a privacy policy and data-breach response plan, can assist an entity to embed good information handling practices and to respond effectively in the event that personal information is misused, 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 confidential information, such as commercially sensitive information, that is not protected by the Privacy Act but is nevertheless important to an entity's functions and activities.

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

Entities that handle personal information should build privacy into their processes, systems, products and initiatives at the design stage. Building privacy into data handling practices from the start, rather than 'bolting it on' at a later stage is known as 'privacy by design'.

The 'privacy by design' stage should also address personal information security, including the appropriateness of technology and the incorporation of 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, 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 information and communications technology (ICT) and electronic records management (ERM) systems.

One way to achieve privacy by design is to conduct a Privacy Impact Assessment (PIA). A PIA is an assessment tool that examines the privacy impacts of a project and assists in identifying ways to minimise those impacts. A PIA will assist in identifying where there are privacy risks, and where additional privacy protections may be required. 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 expects entities to undertake a PIA for any new acts, practices or projects that involve the handling of personal information. 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 the Reform Act, the Commissioner will be able to direct an agency to provide the Commissioner with a PIA.

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 a more detailed information security risk assessment in conjunction with a PIA. This process identifies and evaluates threats and vulnerabilities, including a focus on risks to the privacy of individuals whose personal information the entity handles. It also examines the adequacy of an entity's information security measures in mitigating the risks to information held by the entity (including personal information) and whether those risks should be further mitigated.

Any PIA and information security risk assessment would inform the development of the entity's risk management or information security plans. These plans 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.

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 below 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).

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 and incorporate into their information security practices any industry or technology specific guidance, frameworks or obligations.

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 *Personally Controlled Electronic Health Records Act 2012* (Cth) (e-Health Act).

A list of additional information security resources are at Appendix B.

Circumstances that affect assessment of reasonable steps

What are reasonable steps to ensure information security under the Privacy Act will depend on the circumstances, including the following:

- the nature of the entity holding the personal information
- the nature and quantity of personal information held
- the risk to the individuals concerned if the personal information is not secured
- the data handling practices of the entity holding the information
- the ease with which a security measure can be implemented.

These circumstances (along with relevant examples from recent OAIC investigations) are discussed further below.

Nature of the entity

In determining the steps that it is reasonable for an entity to take to protect its holdings of personal information, the nature of the entity itself is relevant. Factors include the size of the entity and the business model on which the entity operates. For instance, if an entity operates through franchises or dealerships, or gives database and network access to contractors, the steps that it is reasonable for it to take may differ from the steps that it is reasonable for a centralised entity to take.

On 10 January 2011, the Privacy Commissioner 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 data security risk. For this reason, in the Privacy Commissioner'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 obligations under NPP 4.1.

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

Nature and quantity of personal information held

The nature and quantity of personal information held by an entity will affect the steps that it is reasonable for that entity to take.

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 additional restrictions in the Privacy Act concerning the handling of sensitive information by organisations.

Although it is not classed as sensitive information in the Privacy Act, people often expect that their financial information will be given a high level of protection. Generally, as the quantity, extent and sensitivity of personal information held increases, so too will the steps that it is reasonable for that entity to take to protect that information.

On 5 July 2010 the Privacy Commissioner opened an investigation of the Professional Services Review Agency (PSR), which holds Medicare Benefits Program (MBP) and Pharmaceutical Benefits Program (PBP) claims information. It was alleged that PSR was holding medical records in an unsecured manner. During the investigation PSR provided information about the different measures it has in place to keep information secure. In particular, the Commissioner noted that PSR:

- retains records in accordance with the National Archives of Australia guidelines, Normal Administrative Practice and existing Records Authorities
- destroys records in accordance with the timeframes set by the National Archives of Australia and mechanisms set by the PSM and ISM guidelines
- commissioned a review of its information and communication technologies in 2009 to ensure it was achieving best practice standards, and a Records Management Program was undertaken as a result of this review
- undertook a Protective Security Assessment of its practices and undertakes an annual Strategic Risk Assessment as part of its wider audit and compliance regime.

PSR has policy documents that set out how it manages data security including its Privacy Policy, Breach of Code of Conduct Policy and Clear Desk Policy. Some of the practical data security measures flowing from these policies include PSR's secure office environment, its ICT audit logs and tracking program. Based on the information that PSR provided, the Commissioner was satisfied that PSR's practices are consistent with its obligations under IPP 4.

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

Risk

When entities are assessing the steps that they take to protect personal information in their possession, they should consider the risk to the individuals concerned if the information is not secured. For instance, individuals may suffer reputational harm if information becomes public, or material harm if the information exposed enables identity theft or fraud. The likelihood of this harm eventuating will influence whether it is reasonable to take a particular step.

On 20 July 2011, the Privacy Commissioner 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 Webstore 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.

Data handling practices

When determining the appropriate steps to protect personal information, entities should consider the ways in which they handle data. This may include considering how personal information is collected, processed and stored. An entity should also consider whether it outsources any of its data handling. If an entity outsources data handling to a third party, it will need to consider how the third party handles and secures the information. Relevant factors include whether those suppliers are subject to the Privacy Act.

Appropriate steps should be taken to ensure third parties meet the entity's Privacy Act obligations. Appropriate steps may include having specific obligations about the handling of personal information in contracts and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements and conducting inspections of the third party's facilities. 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.

Section 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 IPP. 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.

In July 2011, the Privacy Commissioner published a report on his investigation of Telstra after a mailing list error had resulted in approximately 60,300 letters with incorrect addresses being mailed out. The letters had been sent on Telstra's behalf by a mailing house to contact customers about Telstra's fixed-line phone service. In response to the questions raised by the OAIC, Telstra advised that it had a range of security measures in place to protect customer personal information involved in mail campaigns. These include:

- having an agreement with the mail house that includes privacy and confidentiality obligations
- conducting privacy impact assessments at the outset of mail-out initiatives that use personal information
- a series of approvals before a mail-out process can begin
- procedures to ensure staff handle personal information appropriately during the mail campaign process, including quality control procedures for creating mailing lists.

In this case, despite these measures being in place, an employee inadvertently used the wrong data table, which resulted in inaccurate address information being recorded on a campaign mailing list.

The Privacy Commissioner concluded that Telstra was not in breach of NPP 4 as he was satisfied that this incident occurred due to human error rather than any systemic failure of Telstra's processes or procedures.

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

Ease of implementation

The ease with which a security measure can be implemented will influence the reasonableness of taking that step. It may not be reasonable to implement a measure if doing so will be impracticable or unduly expensive when balanced against the risks.

Additionally, it may not be reasonable to implement a measure if doing so might result in privacy infringements. For example, requiring users to supply extensive personal information to identify themselves prior to accessing their records may result in the entity collecting personal information that it would not otherwise require.

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 if that information is lost, altered, or inappropriately accessed, used, or disclosed. Similarly, entities must balance the taking of steps to prevent disclosure of personal information to someone other than the individual concerned with the right of individuals to access their own personal information.

In 2009, the Privacy Commissioner 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 Commissioner 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 Commissioner 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 Commissioner determined that, following the implementation of these measures, the medical centre met its obligations under NPP 4 and closed her investigation.

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

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 could include taking steps and implementing strategies to manage the following:

- governance
- ICT security
- data breaches
- physical security
- personnel security and training
- workplace policies
- the information life cycle
- standards
- regular monitoring and review.

This section outlines examples of key steps and strategies an entity could take in order to protect personal information and satisfy the 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, after a privacy breach occurs, if an entity becomes aware that security measures which previously protected data are no longer adequate or the entity handles data in a new way.

Entities should consider undertaking a Privacy Impact Assessment and an information security risk assessment for new acts or practices, or changes in existing acts or practices that involve the handling of personal information, 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 an exhaustive set of information security measures. 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).

The OAIC also expects that entities be fully aware of all the personal information they handle, where it is kept and the risks associated with that information. Therefore, it is recommended that entities undertake robust information asset management by developing and maintaining an inventory or register 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 robust information asset management and effective information governance (see 'Governance' section below), it is recommended that Australian Government agencies and more generally entities (as a model of best practice) consult the OAIC's *Open public sector information: from principles to practice* (February 2013).

Although it is not necessary for all entities to take all the steps and strategies outlined below, the OAIC will refer to this guide when assessing an entities compliance with its security obligations in the Privacy Act.

Governance

Entities should establish clear procedures and lines of authority for decisions regarding information security. Entities should 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.

- What governance arrangements does the entity have in place to implement and maintain its information security plans and measures?
- Do the governance arrangements promote awareness and compliance with the information security and privacy obligations that apply to the entity?

ICT security

Effective ICT security requires protecting both computer hardware (the physical devices that make up a computer system) as well as the data that the computer hardware holds from unauthorised use, access, theft or damage. However, ICT security measures should also ensure that the hardware and the data 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.

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, apps, 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 entities to protect themselves against attacks by malicious hackers 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.

ICT security measures can also guard against information not being easily accessible for legitimate use, as well as 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)
- hardware or software malfunctions
- power failure
- 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 be 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 though 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?

Access

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

- 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?
- Is the number of users with administrative privileges limited to the number necessary to enable the entity to carry out its functions and activities?
    - Is access revoked promptly when no longer required?

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.

- 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 or passphase complexity enforced? For example uppercase, lowercase, special character, numeric.
    - 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 there policies in place to prevent the unauthorised downloading, transferring or theft of bulk data through the use of personal storage devices?
- What means exist to identify inappropriate access of files or databases which contain personal information?
- What points of access (eg access to devices, files, networks, databases, 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?
- Are screensaver 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?

Under the Privacy Act, entities must give individuals access to the personal information held about them. Individuals are also able to request correction of the personal information held about them.[3]

- 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 by phone or in person?
    - What measures does the entity take to ensure that these verification processes do not infringe customer/ client privacy?

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.

- 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?
- 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 (eg 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.

3 Along with the right to apply for access under the Privacy Act, individuals have enforceable rights under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to their personal information held by Australian Government agencies. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

- Does the entity maintain an intrusion detection system that includes intrusion detection mechanisms and analysis of event logs?

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 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, has a PIA and information security risk assessment been undertaken to assess the personal information flows caused by the testing? Does the entity's privacy policy reflect the use of personal information for testing?
    - If testing identifies weaknesses, how is this reported and addressed?

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?
- Does the entity review its backups to check that personal information that is no longer needed is deleted? How far back is data recoverable?
- Are backups stored remotely to protect from natural disasters?
- Are backups stored securely to protect against unauthorised access, use or disclosure of personal information?

Communications security

Personal information can be vulnerable to being improperly accessed or disclosed when it is transmitted. For example, personal information may be disclosed if it is left on a fax machine or printer or discussed over the telephone in an open office.

- Are staff made aware of the risks of disclosure and how to mitigate against them 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?

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?

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?
- Has 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?
    - Is 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?
    - How are staff informed of changes to policy and procedures or other workplace security requirements?
- 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 recognising and avoiding 'phishing' and 'spear phishing' attacks and social engineering?

'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 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 (eg in files) is returned?
    - At what time is physical and ICT access revoked?

Workplace policies

Privacy protections have the best chance of being effective if they are integrated into workplace policies. Policies should be regularly monitored and reviewed to ensure that they are effective.

Information security, including appropriate handling of personal information, may be addressed in a single policy document or in a number of separate documents. Additionally, entities should ensure that staff are trained regarding their responsibilities.

- Are there documented policies that address security matters, such as physical, ICT security and other appropriate information handling practices?
    - Are all staff, including short-term staff and contractors, able to access the policy easily?
    - Are mechanisms in place for ensuring that the policy is updated and reviewed? For example, are regular reviews scheduled? Do designated staff members have responsibility for maintaining the policy?
    - Are mechanisms in place to enable staff members to seek clarification of the policy or suggest updates?
    - Are staff reminded to refer to the policy and informed of updates as they occur?
    - How does the entity ensure that the policy is being observed?
    - Does the policy 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 policy?
- 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 (eg password protection, encryption)?
    - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices such as BYODs?
    - 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?

Managing the information life-cycle

Entities that handle personal information as part of their functions and activities need to take reasonable steps to ensure that information is not inappropriately used or disclosed during its lifecycle. This includes ensuring that personal information is not mistakenly disclosed to the incorrect individual, that information is not lost and that it is disposed of appropriately when it is no longer required. Entities may be required by law, including the *Archives Act 1983* (Cth), to retain personal information for a specified period.

Additionally, entities that pass personal information to a third party for storage, processing, or destruction should consider what steps are required to ensure that the third party will protect that information.

- 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 assessed at an early stage to identify whether they raise any privacy issues?
    - Are mitigation strategies recommended by any PIA or information security risk assessment implemented, for example through the development of information security risk management plans?
    - Are those strategies reviewed after a period following implementation to assess whether they are effective?
- Does the entity review its collection practices at appropriate intervals to ensure that unnecessary personal information is not collected or retained?
    - 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? (also see 'Access' section above) 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 data loss?
    - Does the entity have a data contingency plan that incorporates system back-ups? How is the system backed up, and how often?
    - Does the entity have a data contingency plan that incorporates disaster recovery?

- Is processing, storage or other handling of personal information outsourced 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?
- Is there a policy outlining when and how to dispose of personal information when it is no longer required to be retained for a lawful purpose?
    - What steps does the entity take to securely dispose of personal information when it is no longer required?
    - Are staff informed of document destruction procedures?
    - 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 (see above)?
    - How is compliance with data destruction procedures monitored and enforced?
    - How does the entity ensure that data has been permanently deleted from electronic devices prior to disposal?

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)[4], which is relevant to the health sector) or practices, such as electronic funds transfers.

4 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/connecting-australia/ehealth-information-security.

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 27000 series of information security management systems standards and the AS/NZS ISO 31000 of risk management standards. [5]

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. 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?

Regular monitoring and review

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 of information security measures is crucial. The steps and strategies outlined above 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.

- Does the entity regularly monitor and review the operation and effectiveness of its information security measures?
- Are changes implemented as a result of regular monitoring and reviews?

5 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.

Appendix A – Information security obligations in the Privacy Act

Privacy Principles

Information Privacy Principle 4 — Storage and security of personal information

A record keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonable within the power of the record keeper is done to prevent unauthorised use or disclosure of information contained in the record.

National Privacy Principle 4 — Data security

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

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

Part IIIA — Credit reporting

Section 18G — Accuracy and security of credit information files and credit reports

A credit reporting agency in possession or control of a credit information file, or a credit provider or credit reporting agency in possession or control of a credit report, must:

(a) take reasonable steps to ensure that personal information contained in the file or report is accurate, up to date, complete and not misleading; and

(b) ensure that the file or report is protected, by such security safeguards as are reasonable in the circumstances, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(c) if it is necessary for the file or report to be given to a person in connection with the provision of a service to the credit reporting agency or credit provider, ensure that everything reasonably within the power of the credit reporting agency or credit provider is done to prevent unauthorised use or disclosure of personal information contained in the file or report.

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 B – Additional information security resources

OAIC resources

- *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
- *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 Impact Assessment Guide* 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 provides information to all Australians and Australian businesses on how to better protect their information technology environment from cyber based threats and vulnerabilities. CERT Australia is the initial point of contact for cyber security incidents impacting upon Australian networks
- international standards published by the International Standards Organisation and Australian standards published by Standards Australia (see 'Standards' section of this guide)
- *Control Objectives for Information and Related Technology* (COBIT), which is an international framework created by ISACA for information technology (IT) management and IT governance
- *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 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
- 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 Government Information Management Office, assists Australian Government agencies and state jurisdictions in authenticating the identity of another party to a desired level of assurance or confidence.

Office of the Australian Information Commissioner

GPO Box 2999 Canberra ACT 2601
GPO Box 5218 Sydney NSW 2001

For further information
tel: 02 9284 9800 or
enquiries line: 1300 363 992
email: enquiries@oaic.gov.au

or visit our website at
www.oaic.gov.au