Data breach notification guide:
A guide to handling personal information security breaches

August 2014
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.

Date of initial publication: August 2008, revised August 2014


Creative Commons

With the exception of the Commonwealth Coat of Arms, this document titled Data breach notification: a guide to handling personal information security breaches by the Office of the Australian Information Commissioner is licenced under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/deed.en).

This publication should be attributed as: Office of the Australian Information Commissioner, Data breach notification guide: A guide to handling personal information security breaches — August 2014.

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

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Tel: 02 9284 9800
TTY: 1800 620 241 (no voice calls)
Email: enquiries@oaic.gov.au
Contents

Key messages ............................................................................................................................................. 1
Key terms ....................................................................................................................................................... 2
Background ..................................................................................................................................................... 3
The purpose of this guide ............................................................................................................................... 3
Scope of this guide .......................................................................................................................................... 3
Who should use this guide? ......................................................................................................................... 4
Data breaches ................................................................................................................................................ 5
How do data breaches occur? ......................................................................................................................... 5
Preventing data breaches — obligations under the Privacy Act ................................................................. 5
Other obligations ........................................................................................................................................... 6
Considerations for keeping information secure .......................................................................................... 6
Why data breach notification is good privacy practice ............................................................................. 9
The role of the Office of the Australian Information Commissioner ...................................................... 9
Responding to data breaches: four key steps ............................................................................................... 12
STEP 1: Contain the breach and do a preliminary assessment ................................................................. 13
STEP 2: Evaluate the risks associated with the breach .............................................................................. 16
STEP 3: Notification ................................................................................................................................... 22
STEP 4: Prevent future breaches ................................................................................................................. 31
Responding to a large scale data breach: An illustration of how to work through the Four Key Steps .......... 34
Reporting a data breach to the Office of the Australian Information Commissioner .................................. 38
What the OAIC can do................................................................................................................................... 38
What the OAIC cannot do .............................................................................................................................. 38
What to put in a notification to the OAIC ..................................................................................................... 39
How to contact the OAIC .............................................................................................................................. 39
Data breach response process ..................................................................................................................... 41
Appendix A – APP 11 ................................................................................................................................... 42
Appendix B – Contact list: State and territory privacy contacts ................................................................. 43
Key messages

- This guide provides general guidance for agencies and organisations when responding to a data breach involving personal information that they hold.

- Agencies and organisations have obligations under the Privacy Act 1988 (Cth) to put in place reasonable security safeguards and to take reasonable steps to protect the personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

- Those reasonable steps may include the preparation and implementation of a data breach policy and response plan (that includes notifying affected individuals and the OAIC).

- Data breaches are not limited to malicious actions, such as theft or ‘hacking’, but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure.

- In general, if there is a real risk of serious harm as a result of a data breach, the affected individuals and the OAIC should be notified.

- Notification can be an important mitigation strategy for individuals, and can promote transparency and trust in the organisation or agency.

- Notification of a data breach supports good privacy practice.

- Notification of a data breach in compliance with this guide is not required by the Privacy Act. However, the steps and actions in this guide are highly recommended by the OAIC.

- The ALRC has recommended that the Privacy Act be amended to impose a mandatory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach that could give rise to a real risk of serious harm to affected individuals. The operation of this guide could inform the Australian Government’s response to the ALRC’s recommendation that mandatory breach notification be introduced into law.
Key terms

ALRC means the Australian Law Reform Commission.

APPs means the Australian Privacy Principles set out Schedule 1 to the Privacy Act, which apply to APP entities.

APP entity has the meaning set out in s6 of the Privacy Act, and means an agency or organisation for the purpose of the Privacy Act.

Agency has the meaning set out in s6 of the Privacy Act and includes most Australian Government and Norfolk Island departments, agencies and Ministers.

Privacy Act means the Privacy Act 1988 (Cth).

Personal information has the meaning as set out in s6 of the Privacy Act:

- personal information means 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.

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

Note: The Privacy Act regulates the handling of personal information, and does not generally refer to ‘data’. As such, in the interest of consistency with the Act, the previous edition of this guide used the term ‘personal information security breach’.

However, the term ‘data breach’ has since entered into common usage in Australia and in various other jurisdictions. Accordingly, in the interests of clarity and simplicity, this guide uses the term ‘data breach’ rather than ‘personal information security breach’.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s6C 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 ss6D and 6E of the Privacy Act).

TFN means Tax File Number. The Privacy Act includes provisions relating to TFNs in Part III. The OAIC has issued rules under s17 of the Privacy Act to regulate the use of TFNs.

---

Background

The purpose of this guide

This guide was developed to assist agencies and organisations to respond effectively to data breaches.

The OAIC developed this guide in August 2008 in response to requests for advice from agencies and organisations, and in recognition of the global trends relating to data breach notification. In July 2011, the OAIC revised this guide to keep pace with the changing attitudes and approaches to data breach management. In August 2014, the OAIC revised this guide again to take account of amendments to the Privacy Act, including the introduction of the APPs.

In its 2008 report titled ‘For Your Information: Australian Privacy Law and Practice’\(^2\) (Report 108), the ALRC recommended that the Privacy Act be amended to impose a mandatory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach that could give rise to a ‘real risk of serious harm’ to the affected individuals (recommendation 51-1). The OAIC strongly supports that recommendation.

Accordingly, this guide is aimed, in part, at encouraging agencies and organisations to voluntarily put in place reasonable measures to deal with data breaches (including notification of affected individuals and the OAIC), while legislative change is considered by the Government.

Scope of this guide

Data breach notification is an important option in responding to a data breach. However, a key challenge in responding to a data breach is determining if and when notification is an appropriate response.

This guide provides general guidance on key steps and factors for agencies and organisations to consider when responding to a data breach, including notification of breaches.

This guide encourages a risk-analysis approach. Agencies and organisations should evaluate data breaches on a case-by-case basis and make decisions on actions to take according to their own assessment of risks and responsibilities in their particular circumstances.

This guide also highlights the importance of preventative measures as part of a comprehensive information security plan (which may include a data breach response plan).

---

It is not intended that the advice in this guide be limited to data breaches that are breaches of the APPs. Rather, the guide is intended to apply to any situation where personal information has been compromised.

While establishing appropriate thresholds and processes for data breach notification is good privacy practice, the steps and actions outlined in this guide are not specifically required under the Privacy Act. Therefore, while the OAIC strongly recommends compliance with this guide, compliance is not mandatory.

**Who should use this guide?**

This guide has been developed for use by Australian Government and Norfolk Island agencies, and private sector organisations, that handle personal information and are covered by the Privacy Act.

State and territory government agencies, as well as private sector entities not covered by the Privacy Act, may find the guide helpful in outlining good privacy practice. However, the OAIC would not have a role in receiving notifications about data breaches experienced by those entities other than for ACT Government agencies.

State and territory government agencies should also consider the role of relevant Privacy or Information Commissioners (or applicable privacy schemes) in their own jurisdictions (listed at the end of this guide).

---

3 APP11 requires APP entities to take reasonable steps to protect information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure; see Appendix A.
Data breaches

How do data breaches occur?

Data breaches occur in a number of ways. Some examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organisation
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

Preventing data breaches — obligations under the Privacy Act

Security is a basic element of information privacy.4 In Australia, this principle is reflected in the Privacy Act in the APPs

Agencies and organisations are required to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. This requirement is set out in APP 115 (see Appendix A for APP 11).

Sections 20Q and 21S of the Privacy Act imposes equivalent obligations on credit reporting agencies and all credit providers. Similarly, guideline 6.1 of the statutory TFN guidelines6 requires TFN recipients to protect TFN information by such security safeguards as are reasonable in the circumstances.

---

4 See the ‘security safeguards principle’ in the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) available at www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. The Privacy Act was enacted to implement the OECD guidelines in Australia, as recognised in the preamble to the Act.


Depending on the circumstances, those reasonable steps may include the preparation and implementation of a data breach policy and response plan. Notification of the individuals who are or may be affected by a data breach, and the OAIC, may also be a reasonable step (see page 9).

Other obligations

Many agencies are subject to agency-specific legislative requirements that add further protections for personal information (such as secrecy provisions), as well as legislative and other requirements which apply more generally across government. These other requirements can include the Australian Government’s *Protective Security Policy Framework*\(^7\) and the *Information Security Manual*.\(^8\)

Organisations may also be subject to additional obligations through sector-specific legislation in respect of particular information they hold. For example, Part 13 of the *Telecommunications Act 1997* (Cth)\(^9\) sets out obligations on the telecommunications industry in relation to the handling of certain telecommunications-related personal information. Some organisations may also have common law duties relating to the confidentiality of particular information.

These additional obligations need to be considered by agencies and organisations when taking steps to prevent or respond to data breaches.

Considerations for keeping information secure

| Note: Some of the information in Step 4 of this guide (*Prevent future breaches*: see page 31) could equally be used by agencies or organisations as a way of assessing what security measures are necessary to prevent data breaches. |

What are the reasonable steps (as required by APP 11) necessary to secure personal information will depend on context, including (but not limited to):

- the sensitivity (having regard to the affected individual(s)) of the personal information held by the agency or organisation
- the harm that is likely to result to individuals if there is a data breach involving their personal information
- the potential for harm (in terms of reputational or other damage) to the agency or organisation if their personal information holdings are breached, and
- how the agency or organisation stores, processes and transmits the personal information (for example, paper-based or electronic records, or by using a third party service provider).

Appropriate security safeguards for personal information need to be considered across a range of areas. This could include maintaining physical security, computer and network

---


security, communications security and personnel security. To meet their information security obligations, agencies and organisations should consider the following steps:

- **Risk assessment** – Identifying the security risks to personal information held by the organisation and the consequences of a breach of security.

- **Privacy impact assessments** – Evaluating, in a systemic way, the degree to which proposed or existing information systems align with good privacy practice and legal obligations.  

- **Policy development** – Developing a policy or range of policies that implement measures, practices and procedures to reduce the identified risks to information security.

- **Staff training** – Training staff and managers in security and fraud awareness, practices and procedures and codes of conduct.

- **The appointment of a responsible person or position** – Creating a designated position within the agency or organisation to deal with data breaches. This position could have responsibility for establishing policy and procedures, training staff, coordinating reviews and audits and investigating and responding to breaches.

- **Technology** – Implementing privacy enhancing technologies to secure personal information held by the agency or organisation, including through such measures as access control, copy protection, intrusion detection, and robust encryption.

- **Monitoring and review** – Monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures, and ensuring that effective complaint handling procedures are in place.

- **Standards** – Measuring performance against relevant Australian and international standards as a guide.

- **Appropriate contract management** – Conducting appropriate due diligence where services (especially data storage services) are contracted, particularly in terms of the IT security policies and practices that the service provider has in place, and then monitoring compliance with these policies through periodic audits.

---


12 See, for example, [www.standards.org.au](http://www.standards.org.au), or [www.iso.org/iso/home.htm](http://www.iso.org/iso/home.htm).

Further, in seeking to prevent data breaches, agencies and organisations should consider their other privacy obligations under the APPs. Some breaches or risks of harm can be avoided or minimised by not collecting particular types of personal information or only keeping it for as long as necessary. Consider the following:

- **What personal information is it necessary to collect?** – Personal information that is never collected, cannot be mishandled. APP 3 requires that APP entities must not collect personal information unless it is reasonably necessary, or directly related to, one or more of their functions or activities. Additional restrictions apply to the collection of sensitive information (see APP 3.3).

- **How long does the personal information need to be kept?** – APPs 4.3 and 11.2 require APP entities organisations to take reasonable steps to destroy information, on ensure that it is de-identified, if that information is no longer needed for any purpose permitted under the APPs.

Agencies have record-keeping obligations with respect to Commonwealth records – this is reflected in APP 11.2(c). Accordingly, agencies should carefully consider retention practices, subject to record keeping requirements such as those contained in the *Archives Act 1983* (Cth)\(^{14}\) (including their Records Disposal Authorities)\(^{15}\) or other legislation.

---


Why data breach notification is good privacy practice

Notifying individuals when a data breach involves their personal information supports good privacy practice, for the following reasons:

- **Notification as a reasonable security safeguard** – As part of the obligation to keep personal information secure, notification may, in some circumstances, be a reasonable step in the protection of personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (as required by APP 11).

- **Notification as openness about privacy practices** – Being open and transparent with individuals about how personal information may be handled is recognised as a fundamental privacy principle.\(^\text{16}\) Part of being open about the handling of personal information may include telling individuals when something goes wrong and explaining what has been done to try to avoid or remedy any actual or potential harm.\(^\text{17}\)

- **Notification as restoring control over personal information** – Where personal information has been compromised, notification can be essential in helping individuals to regain control of that information. For example, where an individual’s identity details have been stolen, once notified, the individual can take steps to regain control of their identity information by changing passwords or account numbers, or requesting the reissue of identifiers.

- **Notification as a means of rebuilding public trust** – Notification can be a way of demonstrating to the public that an agency or organisation takes the security of personal information seriously, and is working to protect affected individuals from the harms that could result from a data breach. Customers may be reassured to know that an agency or organisation’s data breach response plan includes notifying them, the OAIC, and relevant third parties.

The OAIC strongly encourages notification in appropriate circumstances as part of good privacy practice, and in the interest of maintaining a community in which privacy is valued and respected.

The role of the Office of the Australian Information Commissioner

A data breach may constitute a breach of information security obligations under the Privacy Act; for example, the obligations imposed by the APPs, the TFN guidelines, or the credit reporting provisions of the Act. In those circumstances, the breach will be an

\(^{16}\) See the ‘openness principle’ in the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), available at [www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html). This principle is reflected in APP 1 in the Privacy Act.

\(^{17}\) Agencies may also wish to consider Principle 2: Engaging the community set out in OAIC’s *Principles on open public sector information: Report on review and development of principles* (see footnote 11).
interference with an individual’s privacy.18 Individuals can complain about such interferences to the OAIC.

The OAIC has the function of investigating possible breaches of the Privacy Act. It also has the function of providing guidance and advice to agencies and organisations on the operation of the Privacy Act.19 As such, the OAIC may provide general information on how to respond to a data breach.

Step 3(d) of this guide provides guidance on when it may be appropriate to notify the OAIC of a data breach. Consistent with its statutory functions, the OAIC may consider whether it needs to investigate the conduct. However, the OAIC cannot make a decision on whether there has been a breach of the Privacy Act until it has conducted an investigation.

If an individual thinks an agency or organisation covered by the Privacy Act has interfered with his or her privacy, and they have been unable to resolve the matter directly with the agency or organisation, they can complain to the OAIC.20 The OAIC may investigate21 and may attempt to resolve the matter by conciliation between the parties.

The Commissioner also has the power to initiate an investigation on their own initiative in appropriate circumstances without first receiving a complaint.22

The Commissioner has a range of enforcement powers, including the power to:

- make a determination requiring the payment of compensation for damages or other remedies,23 such as the provision of access or the issuance of an apology (enforceable by the Federal Court or Federal Magistrates Court)
- accept an enforceable undertakings,24
- seek civil penalties of up to or apply for civil penalty orders of up to $340,000 for individuals and up to $1.7 million for companies,25 and
- seek an injunction regarding conduct that would contravene the Privacy Act.26

Deliberate contraventions of some of the credit reporting provisions in Part IIIA of the Privacy Act carry specific penalties.

---

18 See s13 of the Privacy Act
19 See ss 28 and 28B of the Privacy Act.
20 For more information about complaints, see the OAIC’s website: www.oaic.gov.au/privacy/privacy-complaints.
21 See s 40(1) of the Privacy Act.
22 See s 40(2) of the Privacy Act.
23 See s 52 of the Privacy Act.
24 See s 33E of the Privacy Act.
25 See ss 13G and 80W(5) of the Privacy Act.
26 See s 98 of the Privacy Act.
Agencies should also be aware that, under s28B(1)(b) of the Privacy Act, the Information Commissioner can inform the Minister responsible for the Privacy Act of action that needs to be taken by an agency in order to comply with the APPs.

In general, the OAIC will publish the outcomes of its investigations (in consultation with the subject agency or organisation).

In some circumstances, consistent with its roles of education and enforcement, the OAIC may publicise information about the information management practices of an agency or organisation.
Responding to data breaches: four key steps

Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

| Step 1: Contain the breach and do a preliminary assessment |
| Step 2: Evaluate the risks associated with the breach |
| Step 3: Notification |
| Step 4: Prevent future breaches |

There are four key steps to consider when responding to a breach or suspected breach:

Each of the steps is set out in further detail below.

A chart summarising the data breach response process is set out at page 41. Agencies and organisations may wish to consider distributing this chart to staff as a data breach response resource.

General tips:

- Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.
- Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- Agencies and organisations should undertake steps 1, 2 and 3 either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- The decision on how to respond should be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, agencies and organisations may choose to take additional steps that are specific to the nature of the breach.
STEP 1: Contain the breach and do a preliminary assessment

Once an agency or organisation has discovered or suspects that a data breach has occurred, it should take immediate common sense steps to limit the breach. These may include the following:

Contain the breach
Take whatever steps possible to immediately contain the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.

For example, if it is detected that a customer’s bank account has been compromised, can the affected account be immediately frozen and the funds transferred to a new account?

Initiate a preliminary assessment
Move quickly to appoint someone to lead the initial assessment. This person should have sufficient authority to conduct the initial investigation, gather any necessary information and make initial recommendations. If necessary, a more detailed evaluation may subsequently be required.

Determine whether there is a need to assemble a team that could include representatives from appropriate parts of the agency or organisation.

Consider the following preliminary questions:

- What personal information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to affected individuals) that could potentially be caused by the breach?
- How can the breach be contained?

Consider who needs to be notified immediately
Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.

In some cases it may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals).
Escalate the matter internally as appropriate, including informing the person or group within the agency or organisation responsible for privacy compliance.

It may also be appropriate to report such breaches to relevant internal investigation units.

If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police.

If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the OAIC. The OAIC may be able to provide guidance and assistance.

For more information on what the OAIC can and cannot do, see page 38.

Other matters

Where a law enforcement agency is investigating the breach, consult the investigating agency before making details of the breach public.

Be careful not to destroy evidence that may be valuable in determining the cause or would allow the agency or organisation to take appropriate corrective action.

Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.

An example of breach containment and preliminary assessment

An online recruitment agency accepts résumés from jobseekers and makes these available to recruiters and employers on a password protected website.

Jane, a jobseeker whose résumé is on the website, receives an email which she suspects is a ‘phishing’ email. The email is personalised and contains information from her résumé. It contains a number of spelling mistakes and offers her a job. The email claims that all Jane has to do to secure the job is to provide her bank account details so she can be paid. Jane advises the recruitment agency of her suspicions, and forwards a copy of the email to the recruitment agency.

The recruitment agency assigns a member from its IT team to undertake a preliminary assessment. It is found that the email is indeed a phishing email. It claims to be from a recruiter and directs the recipient to a website which asks them to enter further information. It also installs spyware on the recipient’s computer.

The recruitment agency attempts to establish how phishers came to have the résumé details of the jobseeker. The recruitment agency’s preliminary assessment reveals that the phishers have stolen legitimate user names and passwords from recruiters who use the agency’s website and have fraudulently accessed jobseeker information.

The IT team escalates the issue internally by informing senior staff members and quickly contains the breach by disabling the compromised recruiter accounts. Based on the IT
team’s preliminary assessment, senior staff move to evaluate risks associated with the breach and consider what actions should be taken to mitigate any potential harm.
STEP 2: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, agencies and organisations should assess the risks associated with the breach.

Consider the following factors in assessing the risks:

(a) The type of personal information involved.
(b) The context of the affected information and the breach.
(c) The cause and extent of the breach.
(d) The risk of serious harm to the affected individuals.
(e) The risk of other harms.

(a) Consider the type of personal information involved

Does the type of personal information that has been compromised create a greater risk of harm?

Some information is more likely to cause an individual harm if it is compromised, whether that harm is physical, financial or psychological.

For example, government-issued identifiers such as Medicare numbers, driver’s licence and health care numbers, health information, and financial account numbers such as credit or debit card numbers might pose a greater risk of harm to an individual than their name or address.

Also, a combination of personal information typically creates a greater risk of harm than a single piece of personal information.

It may also matter whether the information is permanent or temporary. Permanent information, such as someone’s name place and date of birth, or medical history cannot be ‘re-issued’.

The permanence of the information may be more significant if it is protected by encryption – over time, encryption algorithms may be broken, so such information may be at greater longer term risk of being compromised. On the other hand, temporary information may have changed by the time it has been decrypted.

Who is affected by the breach?

Employees, contractors, the public, clients, service providers, other agencies or organisations?

Remember that certain people may be particularly at risk of harm. A data breach involving name and address of a person might not always be considered high risk. However, a breach to a women’s refuge database containing name and address information may expose women who attend the refuge to a violent family member. There may be less risk if the breach only relates to businesses that service the refuge.
(b) Determine the context of the affected information and the breach

**What is the context of the personal information involved?**

For example, a list of customers on a newspaper carrier’s route may not be sensitive information. However, the same information about customers who have requested service interruption while on vacation may be more sensitive.

The sensitivity of personal information that may also publicly available information (such as the type found in a public telephone directory) also depends on context. For example, what might be the implications of someone’s name and phone number or address being associated with the services offered, or the professional association represented?

*What parties have gained unauthorised access to the affected information?*

To whom was the information exposed? Employee records containing information about employment history such as performance and disciplinary matters or a co-worker’s mental health might be particularly sensitive if exposed to other employees in the workplace and could result in an individual being the subject of humiliation or workplace bullying.

*Have there been other breaches that could have a cumulative effect?*

A number of small, seemingly insignificant, breaches could have a cumulative effect. Separate breaches that might not, by themselves, be assessed as representing a real risk of serious harm to an affected individual, may meet this threshold when the cumulative effect of the breaches is considered.

This could involve incremental breaches of the same agency or organisation’s database. It could also include known breaches from a number of different sources.

*How could the personal information be used?*

Could the information be used for fraudulent or otherwise harmful purposes, such as to cause significant embarrassment to the affected individual?

Could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

(c) Establish the cause and extent of the breach

*Is there a risk of ongoing breaches or further exposure of the information?*

What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
Is there evidence of theft?

Is there evidence that suggests theft, and was the information the target? For example, where a laptop is stolen, can it be determined whether the thief specifically wanted the information on the laptop, or the laptop hardware itself?

Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as law enforcement.

Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?

Is the information rendered unreadable by security measures that protect the stored information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?

For example, if a laptop containing adequately encrypted information is stolen, but is subsequently recovered and investigations show that the information was not accessed, copied or otherwise tampered with, notification to affected individuals may not be necessary.

What was the source of the breach?

For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does the information seem to have been lost or misplaced?

The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.

For example, the client may have a common surname which leads a staff member to accidentally access the wrong client record. The access records show that the staff member immediately closed the client record once they became aware of their mistake. The risk of harm will be less in this case than in the case where a staff member intentionally and deliberately opens a client’s record to browse the record, or to use or disclose that information without a legitimate business reason for doing so.

Has the personal information been recovered?

For example, has a lost laptop been found or returned? If the information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?

What steps have already been taken to mitigate the harm?

Has the agency or organisation contained the breach? For example, have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?

Is this a systemic problem or an isolated incident?

When checking the source of the breach, it is important to check whether any similar breaches have occurred in the past. Sometimes, a breach can signal a deeper problem
with system security. This may also reveal that more information has been affected than initially thought, potentially heightening the awareness of the risk posed.

**How many individuals are affected by the breach?**

If the breach is a result of a systemic problem, there may be more people affected than first anticipated.

Even where the breach involves accidental and unintentional misuse of information, if the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The agency or organisation’s response should be proportionate.

While the number of affected individuals can help gauge the severity of the breach, it is important to remember that even a breach involving the personal information of one or two people can be serious, depending on the information involved.

**(d) Assess the risk of harm to the affected individuals**

**Who is the recipient of the information?**

Is there likely to be any relationship between the unauthorised recipients and the affected individuals?

For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Was the disclosure to a person against whom the individual has a restraining order, or to co-workers who have no need to have the information?

Or was the recipient a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it? For example, was the information sent to the individual’s lawyer instead of being sent to them, or to another party bound by professional duties of confidentiality or ethical standards?

**What harm to individuals could result from the breach?**

Examples include:

- identity theft
- financial loss
- threat to physical safety
- threat to emotional wellbeing
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships, or
- workplace or social bullying or marginalisation.
(e) Assess the risk of other harms

Other possible harms, including to the agency or organisation that suffered the breach

Examples include:

- the loss of public trust in the agency, government program, or organisation
- reputational damage
- loss of assets (e.g., stolen computers or storage devices)
- financial exposure (e.g., if bank account details are compromised)
- regulatory penalties (e.g., for breaches of the Privacy Act)
- extortion
- legal liability, and
- breach of secrecy provisions in applicable legislation.

An example of evaluating the risks associated with the breach

A newspaper publisher receives a call from a newsagent that sells its newspapers. The newsagent says that the address labels on the bundles of newspapers delivered to his shop appear to show subscriber information printed on the other side. The information includes names, addresses and credit card details.

Following a preliminary investigation, the newspaper publisher confirms that some labels have been inadvertently printed on the back of subscriber lists.

As a first step to containing the breach, the publisher attempts to contact newsagencies that have received the newspapers and asks them to check the labels on the bundles and securely destroy any that show subscriber details on the back.

With these first steps completed, the newspaper publisher begins to evaluate the risks associated with the breach.

The information that was involved in the breach was name, address and credit card information. The newspaper has a large number of subscribers. Further investigations into the breach are unable to reveal how many subscribers’ details have been exposed.

The bundles of newspapers displaying subscriber information have been delivered to newsagencies in the early hours of the morning. The newspaper publisher notes that the subscriber information was therefore at risk of unauthorised access during the time between delivery and when the newsagents arrived to open shop.

Further investigations reveal that many newsagencies have already discarded the labels before checking could be carried out as to whether they contained subscriber information. This means that, in many cases, the subscriber lists may not have been securely destroyed.
The newspaper publisher concludes that the exposure of this information could present a real risk of serious harm (in this case, financial harm) to many individuals. Based on the conclusion that this is a serious breach, the publisher moves to notify subscribers. Given the large number of potentially affected individuals and the risk of serious financial harm, the publisher also notifies the OAIC, particularly as there is a real possibility that individuals may complain about the breach.

**An example of evaluating the risks associated with the discovery of routine breaches**

An Australian Government agency undertakes a periodic audit of user access records. The audit reveals an unusual pattern of client account enquiries in one branch of the agency. The client records contain address information, financial information, and other details. The enquiries have occurred over a 12 month period.

After some investigation, which includes interviewing the relevant staff, managers and the department head, it is determined that a specific staff member, John, has been browsing the client accounts of his family and friends without any legitimate business purpose (and therefore without authorisation). There is no evidence that client information has been disclosed to any third party.

The agency recognises that some of the information in the client accounts (the financial information in particular) is sensitive information that is not readily available. The agency considers that there is real risk of embarrassment or other harms from the release of that information, especially to a person such as John, who has a personal relationship with the affected individuals and could combine the information with the details about the individuals that he already knows.

On that basis, the agency decides to notify the individuals affected by the unauthorised access. It also takes measures to prevent unauthorised access to client accounts by staff, and to ensure that all staff are aware of their obligations to act appropriately.

The agency considers that, having regard to the sensitivity of the information and the context of the breach, the breach is sufficiently serious to warrant notification to the OAIC.
STEP 3: Notification

Agencies and organisations should consider the particular circumstances of the breach, and:

(a) decide whether to notify affected individuals, and, if so
(b) consider when and how notification should occur, who should make the notification, and who should be notified
(c) consider what information should be included in the notification, and
(d) consider who else (other than the affected individuals) should be notified.

Notification can be an important mitigation strategy that has the potential to benefit both the agency or organisation and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and desensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.

Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves. Agencies and organisations should:

• take into account the ability of the individual to take specific steps to mitigate any such harm, and
• consider whether it is appropriate to inform other third parties such as the OAIC, the police, or other regulators or professional bodies about the data breach.

(a) Deciding whether to notify affected individuals

Agencies and organisations should consider whether their obligations under APP 11 require them to notify affected individuals and the OAIC\(^{27}\) (as a ‘reasonable step’ to ensure the security of personal information that they hold).

The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected individual.

Agencies and organisations should consider the following factors when deciding whether notification is required:

• What is the risk of serious harm to the individual as determined by step 2?
• What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)? For example, would an individual be able to have a new bank account number issued

\(^{27}\) For information on notifying the OAIC, see page 37.
to avoid potential financial harm resulting from a breach? Would steps such as monitoring bank statements or exercising greater vigilance over their credit reporting records assist in mitigating risks of financial or credit fraud?

- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?

- What are the legal and contractual obligations to notify, and what are the consequences of notification?

There may be adverse consequences if an agency or organisation does not notify affected individuals. For example, if the public, including the affected individuals, subsequently find out about the breach through the media, there may be loss of public trust in the agency or organisation (which, in turn, could have its own costs).

(b) Notification process

At this stage, the organisation or agency should have as complete a set of facts as possible and have completed the risk assessment to determine whether to notify individuals. The following tables set out some of the considerations in the notification process.

Sometimes the urgency or seriousness of the breach dictates that notification should happen immediately, before having all the relevant facts.

**When to notify?**

In general, individuals affected by the breach should be notified as soon as reasonably possible.

If law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

Delaying the disclosure of details about a breach of security or information systems may also be appropriate until that system has been repaired and tested or the breach contained in some other way.

**How to notify?**

In general, the recommended method of notification is direct – by phone, letter, email or in person – to the affected individuals.

Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.

Preferably, notification should be ‘standalone’ and should not be ‘bundled’ with other material unrelated to the breach, as it may confuse recipients and affect the impact of the breach notification.

In certain cases, it may be appropriate to use multiple methods of notification.
Agencies and organisations should also consider whether the method and content of notification might increase the risk of harm, such as by alerting the person who stole the laptop of the value of the information on the laptop, if it would not otherwise be apparent.

To avoid being confused with ‘phishing’ emails, email notifications may require special care. For example, only communicate basic information about the breach, leaving more detailed advice to other forms of communication.

Who should notify?
Typically, the agency or organisation that has a direct relationship with the customer, client or employee should notify the affected individuals.

This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate.

Joint and third party relationships can raise complex issues. For example, the breach may occur at a retail merchant but involve credit card details from numerous financial institutions, or the card promoter may not be the card issuer (for example, many airlines, department stores and other retailers have credit cards that display their brand, though the cards are issued by a bank or credit card company). Or the breach may involve information held by a third party ‘cloud’ data storage provider, based outside of Australia.

The issues in play in each situation will vary. Organisations and agencies will have to consider what is best on a case by case basis. However some relevant considerations might include:

- Where did the breach occur?
- Who does the individual identify as their ‘relationship’ manager?
- Does the agency or organisation that suffered the breach have contact details for the affected individuals? Are they able to obtain them easily? Or could they draft and sign off the notification, for the lead organisation to send?

Is trust important to the organisation’s or agency’s activities?

Who should be notified?
Generally, it should be the individual(s) affected by the breach. However, in some cases it may be appropriate to notify the individual’s guardian or authorised representative on their behalf.

There may be circumstances where carers or authorised representatives should be notified as well as, or instead of, the individual.

Where appropriate, clinical judgement may be required where notification may exacerbate health conditions, such as acute paranoia.
(c) What should be included in the notification?

The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Notifications should include the types of information detailed below:

- **Incident Description** — Information about the incident and its timing in general terms. The notice should not include information that would reveal specific system vulnerabilities.

- **Type of personal information involved** — A description of the type of personal information involved in the breach. Be careful not to include personal information in the notification, to avoid possible further unauthorised disclosure.

- **Response to the breach** — A general account of what the agency or organisation has done to control or reduce the harm, and proposed future steps that are planned.

- **Assistance offered to affected individuals** — What the agency or organisation will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.

  For example, whether the agency or organisation can arrange for credit monitoring or other fraud prevention tools, or provide information on how to change government issued identification numbers (such as a driver’s licence number).

- **Other information sources** — Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy.


- **Agency/ Organisation contact details** — Contact information of areas or personnel within the agency or organisation that can answer questions, provide further information or address specific privacy concerns.

  Where it is decided that a third party will notify of the breach, a clear explanation should be given as to how that third party fits into the process and who the individual should contact if they have further questions.

- **Whether breach notified to regulator or other external contact(s)** — Indicate whether the agency or organisation has notified the OAIC or other parties listed in the table at 3(d).

- **Legal implications** — The precise wording of the notice may have legal implications; organisations and agencies should consider whether they should seek legal advice. The legal implications could include secrecy obligations that apply to agencies.

- **How individuals can lodge a complaint with the agency or organisation** — Provide information on internal dispute resolution processes and how the
individual can make a complaint to the agency or organisation or industry complaint handling bodies.28

- **How individuals can lodge a complaint with the OAIC** — If the agency or organisation is covered by the Privacy Act, explain that if individuals are not satisfied with the response by the agency or organisation to resolve the issue, they can make a complaint to the OAIC. The OAIC’s contact details are set out at page 39.

- **How individuals can lodge a complaint with the relevant state or territory privacy or information regulator** — If the agency or organisation is not covered by the Privacy Act, explain how and in what circumstances individuals can lodge a complaint with the relevant regulator. See Appendix B for the contact details of State and Territory regulators.

### (d) Who else should be notified?

In general, notifying the OAIC, or other authorities or regulators should not be a substitute for notifying affected individuals. However, in some circumstances it may be appropriate to notify these third parties:

- **OAIC** — The OAIC strongly encourages agencies and organisations to report serious data breaches to the OAIC. The potential benefits of notifying the OAIC, together with what it can and cannot do about a notification, are set out at page 38.

  - The following factors should be considered in deciding whether to report a breach to the OAIC:
    - any applicable legislation that may require notification
    - the type of the personal information involved and whether there is a **real risk of serious harm** arising from the breach, including non-monetary losses
    - whether a large number of people were affected by the breach
    - whether the information was fully recovered without further disclosure
    - whether the affected individuals have been notified, and
    - if there is a reasonable expectation that the OAIC may receive complaints or inquiries about the breach.

- **Police** — If theft or other crime is suspected. The Australian Federal Police should also be contacted if the breach may constitute a threat to national security.

- **Insurers or others** — If required by contractual obligations.

---

• **Credit card companies, financial institutions or credit reporting agencies** — If their assistance is necessary for contacting individuals or assisting with mitigating harm.

• **Professional or other regulatory bodies** — If professional or regulatory standards require notification of these bodies. For example, other regulatory bodies, such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority have their own requirements in the event of a breach.

• **Other internal or external parties not already notified** — Agencies and organisations should consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards.

  Consider:
  
  o third party contractors or other parties who may be affected
  o internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or
  o union or other employee representatives.

• **Agencies that have a direct relationship with the information lost/stolen** — Agencies and organisations should consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.

---

**An example of notification of affected individuals**

A bank customer, Margaret, receives mail from her bank. When she opens the envelope she notices that correspondence intended for another customer – Diego – has been included in the same envelope. The correspondence includes Diego’s name, address and account details.

Margaret contacts the bank to report the incident. The bank asks that she return the mail intended for Diego to them.

The bank then contacts Diego by phone to notify him of the breach, apologises to him, and advises that it will be investigating the matter to determine how the incident occurred and how to prevent it from reoccurring. The bank also offers to restore the security of Diego’s customer information by closing his existing account and opening a new account. In addition, the bank agrees to discuss with Diego any further action he considers should be taken to resolve the matter to his satisfaction and provides a contact name and number that Diego can use for any further enquiries.
The bank investigates the matter, including getting reports from the mailing house it uses to generate and despatch customer correspondence. While the mailing house has a number of compliance measures in place to manage the process flow, it appears that an isolated error on one production line meant that two customer statements were included in one envelope.

Following its assessment of the breach, the bank is satisfied that this is an isolated incident. However, it reviews the compliance measures taken by the mailing house has in place to ensure they are sufficient to protect customer information from unintentional disclosure through production errors. The bank writes to Diego and informs him of the outcome of its investigation.

An example of notification of affected individuals and the OAIC

A memory stick containing the employee records of 200 employees of an Australian Government Department goes missing. Extensive searches fail to locate the whereabouts of the memory stick. The information contained in the employee records includes the names, salary information, TFNs, home addresses, phone numbers, birth dates and in some cases health information (including disability information) of current staff. The data on the memory stick is not encrypted.

Due to the sensitivity of the unencrypted information – not only the extent and variety of the information, but also the inclusion of health and disability information in the records – the Department decides to notify employees of the breach. Anticipating that individuals may, at some point, complain, it also notifies the OAIC of the breach and explains what steps it is taking to resolve the situation.

A senior staff member emails the affected staff to notify them of the breach. In the notification she offers staff an apology for the breach, explains what types of information were involved, notes that the OAIC has been informed of the breach, and explains what steps have been put in place to prevent this type of a breach occurring in the future. The senior staff member also provides staff with details about how they can have a new TFN issued, and informs staff that they can make a complaint to the OAIC if they are unhappy with the steps the agency has taken.

An example of notification of affected individuals, OAIC and police

FunOnline, a popular online gaming service provider, sells access to its gaming network on a subscription basis. FunOnline collects and holds a range of personal information from its customers in order to create a user account and deal with subscription payments, including names, dates of birth, email addresses, postal addresses, and credit card numbers.

During a routine security check, FunOnline discovers through the use of intrusion detection software that the server containing its account information has been
compromised, and the account information of over 500,000 customers has been accessed without authorisation and, most likely, copied.

FunOnline takes immediate steps to contain the breach (including temporarily shutting down its servers) and notifies the OAIC. Based on its belief that criminal activity has been involved, FunOnline also contacts the police.

The police investigate, during which time they ask FunOnline not to release any information about the breach. FunOnline uses this period to engage a technology security firm to enhance the security of its accounts systems.

As soon as the police are satisfied it will not compromise their investigation, FunOnline notifies the affected customers. FunOnline explains exactly what happened and when, that the police have been investigating, and that the OAIC has been notified. FunOnline also suggests that affected customers monitor their credit card accounts and contact their financial institution if they have any concerns.

An example of no notification

In contravention of policy, a staff member at an Australian Government Department takes a memory stick out of the office so that he can work on some files at home. At some point between leaving work and arriving at home, the staff member loses the memory stick. He reports it missing the next day.

Despite the assistance of the transport authority, the Department is unable to locate the memory stick. The Department conducts a preliminary assessment of the breach, then evaluates the risks associated with the loss of the memory stick.

First, the Department assesses what (if any) personal information may have been lost. While the memory stick did not contain client records, it did contain the names, phone numbers and business email addresses of about 120 external stakeholders involved in a project lead by the Department, along with email correspondence from these stakeholders.

Further evaluation reveals that data held on the stick is protected by high level encryption technology. The Department consults with its IT team to confirm that the encryption on the memory stick is adequately secure and, following confirmation by that team, decides that notification of individuals whose personal information was held on the memory stick is unnecessary.
In contravention of policy, a staff member at an Australian Government Department takes a memory stick out of the office so that he can work on some files at home. At some point between leaving work and arriving at home, the staff member loses the memory stick. He reports it missing the next day.

Despite the assistance of the transport authority, the Department is unable to locate the memory stick. The Department conducts a preliminary assessment of the breach, then evaluates the risks associated with the loss of the memory stick.

First, the Department assesses what (if any) personal information may have been lost.

While the memory stick did not contain client records, it did contain the names, phone numbers and business email addresses of about 120 external stakeholders involved in a project lead by the Department, along with email correspondence from these stakeholders.

Further evaluation reveals that data held on the stick is protected by high level encryption technology. The Department consults with its IT team to confirm that the encryption on the memory stick is adequately secure and, following confirmation by that team, decides that notification of individuals whose personal information was held on the memory stick is unnecessary.

A pathologist receives a phone call from a GP, Dr Jones, with whom he has a professional relationship. Dr Jones advises the pathologist that she has just received a fax from the pathologist’s office disclosing test results for an individual that is not her patient. When the pathologist checks his records, he discovers that the test results were intended for a different GP.

The pathologist asks Dr Jones to destroy the test results and considers whether notification of the patient is warranted.

The pathologist recognises that Dr Jones is bound by ethical duties, and is familiar with principles of confidentiality and privacy. Accordingly, the pathologist is confident that Dr Jones can be relied upon not to mishandle the information contained in the test results and the disclosure is unlikely to pose a serious risk to the privacy of the patient.

The pathologist decides not to notify the patient, but he reviews his practices to avoid a similar breach occurring in the future. The pathologist ensures that administrative staff are trained to exercise care in checking that fax numbers are accurate. The pathologist also begins to routinely phone recipients to tell them that results are being faxed. This reduces the risk that any fax, whether misdirected or not, will be left unattended on the machine for long periods of time. It also allows the intended recipient to let the sender know if a fax not received.
STEP 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, agencies and organisations need to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

This plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).

The plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

Suggested preparations for responding to a data breach include the following:

- Develop a breach response plan — While the aim should be to prevent breaches, having a breach response plan may assist in ensuring a quick response to breaches, and greater potential for mitigating harm.

  The plan could set out contact details for appropriate staff to be notified, clarify the roles and responsibilities of staff, and document processes which will assist the agency or organisation to contain breaches, coordinate investigations and breach notifications, and cooperate with external investigations.

- Establish a breach response team — Depending on the size of the agency or organisation, consider establishing a management team responsible for responding to personal information breaches. The team could include representatives from relevant areas that may be needed to investigate an incident, conduct risk assessments and make appropriate decisions (for example, privacy, senior management, IT, public affairs, legal).

  The team could convene periodically to review the breach response plan, discuss new risks and practices, or consider incidents that have occurred in other agencies or organisations.

  It may also be helpful to conduct ‘scenario’ training with team members to allow them to develop a feel for an actual breach response. Key issues to test in such training would be identifying when notification is an appropriate response, and the timing of that notification.
• **Identify relevant service providers** — Consider researching and identifying **external** service providers that could assist in the event of a data breach, such as forensics firms, public relations firms, call center providers and notification delivery services. The contact details of the service providers could be set out in the breach response plan. This could save time and assist in responding efficiently and effectively to a data breach.

• **Enhance internal communication and training** — Ensure staff have been trained to respond to data breaches effectively, and are aware of the relevant policies and procedures. Staff should understand how to identify and report a potential data breach to the appropriate manager(s).

• **Enhance transparency** — Include information in the agency or organisation’s privacy policy about how it responds to breaches. This could include letting individuals know when and how they are likely to be notified in the event of a breach, and whether the agency or organisation would ask them to verify any contact details or other information.

This would make clear to individuals how their personal contact information is used in the event of a breach, and may also assist individuals to avoid ‘phishing’ scam emails involving fake breach notifications and requests that recipients verify their account details, passwords and other personal information.

**Tips for preventing future breaches**

Some of the measures that have resulted from real-life data breaches include:

• the creation of a senior position in the agency or organisation with specific responsibility for data security

• the institution of a ban on bulk transfers of data onto removable media without adequate security protection (such as encryption)

• disabling the download function on computers in use across the agency or organisation, to prevent the download of data onto removable media

• the institution of a ban on the removal of unencrypted laptops and other portable devices from government buildings

• the institution of a policy requiring the erasing of hard disk drives and other digital storage media (including digital storage integrated in other devices such as multifunction printers or photocopiers) prior to being disposed of or returning to the equipment lessor

• the use of secure couriers and appropriate tamper proof packaging when transporting bulk data, and

• the upgrading of passwords (for example, an increase from 6 to 8 characters, including numbers and punctuation), and the institution of a policy requiring passwords to be changed every 8 weeks.

---

29 Agencies: see footnote 14 re appointing a senior executive ‘information champion’ to be responsible for information management and governance.
Technological advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of data breaches due to the size and portability of these devices, which can be lost or misplaced more easily when taken outside of the office. There is also a risk of theft because of the value of the devices themselves (regardless of the information they contain).

Preventative steps that agencies and organisations can take include conducting risk assessments to determine:

- whether and in what circumstances (and by which staff), personal information is permitted to be removed from the office, whether it is removed in electronic form on DVDs, USB storage devices such as memory sticks, portable computing devices such as laptops, or in paper files, and
- whether their stored data, both in the office and when removed from the office, requires security measures such as encryption and password protection.\(^3^0\)

\(^{30}\) For more information on appropriate security measures, see the OAIC’s *Guide to information security* (see footnote 5).
Responding to a large scale data breach: An illustration of how to work through the Four Key Steps

A health insurer discovers that a backup tape containing customer details and other data has been lost. The information on the tape was not encrypted. The insurer routinely creates two copies of each backup tape. One tape is stored on site; the other tape is stored securely off-site. The lost backup tape was the copy stored on-site and included data collected during the previous month.

Step 1 — Containing the breach and the preliminary assessment

The Chief Executive Officer nominates the Risk & Compliance Manager to lead an investigation. The Risk Manager’s initial assessment suggests that the tapes were lost when the insurer’s IT department moved some records between floors.

The Risk Manager interviews the staff involved in moving the records, reviews the relocation plan and arranges for the building to be searched. Despite these efforts, the tape cannot be found.

The Risk Manager moves on to assessing the breach. She thinks that the breach was most likely the result of poor practices and sloppy handling. However, while there is no evidence that the tape was stolen, theft cannot be ruled out. The type of information that has been lost and how it could be used is an important part of the risk assessment.

Step 2 — Evaluate the risks associated with the breach

The evaluation shows that the information on the tapes falls into 3 main groups:

Group 1 — Enquiry information

- **Type of information** — Enquiry information collected via the website to provide quotes. Only included state, date of birth and gender and was retained for statistical marketing purposes.
- **Identity apparent or ascertainable?** — No. The information is aggregated statistical data only.
- **Sensitivity** — None.
- **How could the information be used?** — The information is likely to be of little or no use other than for statistical purposes
- **Source** — Probably unintentional and accidental. But theft is also a possibility. As the source of the breach is unclear, and given the sensitivity of much of the information, the insurer decides to assume a worst case scenario.
- **Severity** — The information was not encrypted or recovered. The large number of records involved and the sensitivity of the many of the records (health and financial information, as well as identifying information), make this a serious breach.
- **A real risk of serious harm?** — No.
• **Current contact details held?** — No.

**Group 2 — Application information**

- **Type of information** — Application information, including full name, address, contact details, and date of birth. Also includes Medicare card number, and credit card details.
- **Identity apparent or ascertainable?** — Yes.
- **Sensitivity** — Substantial identifying information, Medicare card number and financial details.
- **How could the information be used?** — The information could be used for identity theft and financial fraud. There is a lesser possibility that it could be used to attempt fraud against the Medicare and PBS systems.
- **Source** — Probably unintentional and accidental. But theft is also a possibility. As the source of the breach is unclear, and given the sensitivity of much of the information, the insurer decides to assume a worst case scenario.
- **Severity** — The information was not encrypted or recovered. The large number of records involved and the sensitivity of many of the records (health and financial information, as well as identifying information), make this a serious breach.
- **A real risk of serious harm?** — Yes. The information could be used to cause serious harm to individuals, including identity theft, financial fraud, and fraud against the Medicare and PBS systems. Possibly health fraud.
- **Current contact details held?** — Yes, from current member list and external sources.

**Group 3 — Claims information**

- **Type of information** — Claims information, including full name, member number, contact details, and clinical information about the treatment being claimed.
- **Identity apparent or ascertainable?** — Yes.
- **Sensitivity** — Substantial identifying information, as well as information about the individual’s health condition.
- **How could the information be used?** — The information could be used for identity theft, as well as being potentially embarrassing or stigmatising to the individual.
- **Source** — Probably unintentional and accidental. But theft is also a possibility. As the source of the breach is unclear, and given the sensitivity of much of the information, the insurer decides to assume a worst case scenario.
- **Severity** — The information was not encrypted or recovered. The large number of records involved and the sensitivity of many of the records (health and financial information, as well as identifying information), make this a serious breach.
• **A real risk of serious harm?** — Yes. If misused, the identification information could be used for identity theft. Serious harm could also arise from misuse of the health information, including stigma, embarrassment, discrimination or disadvantage or, in extreme cases, blackmail.

• **Current contact details held?** — Yes, from current member list and external sources.

The evaluation shows that there is a real risk of serious harm for Group 2 and 3 individuals, and that the information in Group 1 is not personal information.

**Step 3 – Notification**

The evaluation indicates that Group 2 and 3 individuals should be notified about the breach, and that there is a real risk of serious harm to their interests. If notified, individuals could take steps to mitigate the risks of identity theft and financial fraud. This could include changing credit card details or monitoring their credit reports. While there may be limited steps that can be taken to mitigate the risks of their health information being mishandled, individuals should still be informed given the heightened sensitivities of this information.

The Risk Manager also considered whether notification would cause harm by leading to unfounded concern or alarm.

Taking all these factors and the evaluation into account, it is decided that individuals in Groups 2 and 3 should be notified. Separate letters are drawn up for each group, outlining the general types of information that are affected.

The Risk Manager also arranges for the notification letters to include:

• a general description of the type of information that has been lost for each group
• what individuals can do to mitigate the harm caused by the breach, and
• who they can call to get further information or assistance.

For example, the notification to individuals in Group 2 tells them that the information they provided on their application form, including their Medicare number and credit card details, may have been compromised. If an individual is concerned about either, they are advised to contact Medicare Australia or their financial institution so as to change their registration and account details. Group 3 individuals are told that a record containing their claims information has been lost, including the clinical details held on their file.

Both letters explain that there is no evidence of theft, and that the company is notifying the individuals as a precautionary measure only.

The notifications also include contact details for the insurer’s customer care area and the OAIC, and suggest that individuals should check their credit card account statements and credit reports for any unusual activity.
The Risk Manager also notes that some claimants had an authorised representative acting for them. These records are separately assessed to determine whether notification should be made to the authorised representative rather than the member.

Staff in the insurer’s customer care area are briefed about the breach and given instructions about how to help customers responding to a notification.

Given the large number of individuals affected, and the sensitive nature of the information, the insurer notifies the OAIC. The insurer explains what steps it has taken to address the breach. It also advises the OAIC of the contact details for the insurer’s customer care area, so that customers contacting the OAIC can be redirected to the insurer if appropriate.

**Step 4 – Preventing Future Breaches**

Once immediate steps have been taken to respond to the breach, the Chief Information Officer (CIO) carries out an audit of the security policies for storage and transfer of backup tapes and reviews the access of staff in the area. The CIO also makes some amendments to the compliance program to ensure non-compliance with IT Security policies will be detected and reported in the future.
Reporting a data breach to the Office of the Australian Information Commissioner

Agencies and organisations are strongly encouraged to notify the OAIC of a data breach where the circumstances indicate that it is appropriate to do so, as set out in Step 3(d). The potential benefits of notifying the OAIC of a data breach may include the following:

- An agency or organisation’s decision to notify the OAIC on its own initiative is likely to be viewed by the public as a positive action. It demonstrates to clients and the public that the agency or organisation views the protection of personal information as an important and serious matter, and may therefore enhance client/public confidence in the agency or organisation.

- It can assist the OAIC in responding to inquiries made by the public and managing any complaints that may be received as a result of the breach. If the agency or organisation provides the OAIC with details of the matter and any action taken to address it, and prevents future occurrences, then, based on that information, any complaints received may be able to be dealt with more quickly. In those circumstances, consideration will need to be given to whether an individual complainant can demonstrate that they have suffered loss or damage, and whether some additional resolution is required. Alternatively, the OAIC may consider that the steps taken have adequately dealt with the matter.

Note: Reporting a breach does not preclude the OAIC from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or on the Commissioner’s initiative).

If the agency or organisation decides to report a data breach to the OAIC, the following provides an indication of what the OAIC can and cannot do:

What the OAIC can do

- Provide general information about obligations under the Privacy Act, factors to consider in responding to a data breach, and steps to take to prevent similar future incidents.

- Respond to community enquiries about the breach and explain possible steps that individuals can take to protect their personal information.

What the OAIC cannot do

- Provide detailed advice about how to respond to a breach, or approve a particular proposed course of action. Agencies and organisations will need to seek their own legal or other specialist advice.

- Agree not to investigate (either using the Commissioner’s power to investigate on their own initiative, or if a complaint is made to the OAIC) if the OAIC is notified of a breach.

When the OAIC receives a complaint about an alleged breach of the Act, in most cases, the OAIC must investigate. As set out above, the OAIC may also investigate an act or
practice in the absence of a complaint on the Commissioner’s initiative. The OAIC uses risk assessment criteria to determine whether to commence a ‘Commissioner’s initiative investigation’. Those criteria include:

- whether a large number of people have been, or are likely to be affected, and the consequences for those individuals
- the sensitivity of the personal information involved
- the progress of an agency or organisation’s own investigation into the matter
- the likelihood that the acts or practices involve systemic or widespread interferences with privacy
- what actions have been taken to minimise the harm to individuals arising from the breach, such as notifying them and/or offering to re-secure their information, and
- whether another body, such as the police, is investigating.

These factors are similar to those included in the risk assessment criteria for responding to a data breach.

**What to put in a notification to the OAIC**

Any notice provided to the OAIC should contain similar content to that provided to individuals (see page 25). It should not include personal information about the affected individuals. It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response the agency or organisation has made to the breach
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person, and
- whether the breach has been notified to other external contact(s).

**How to contact the OAIC**

**Telephone**

1300 363 992 (local call cost, but calls from mobile and payphones may incur higher charges)

**TTY**

1800 620 241 (this number is dedicated for the hearing impaired only, no voice calls)

**Post:**

GPO Box 5218

Sydney NSW 2001
Facsimile
+61 2 9284 9666

Email
enquiries@oaic.gov.au

Website
www.oaic.gov.au
Data breach response process

MAINTAIN INFORMATION SECURITY—APP 11
Protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure. To comply with their obligations under the APPs, agencies and organisations should consider:

- the sensitivity of the personal information
- the harm likely to flow from a security breach
- developing a compliance and monitoring plan, and
- regularly reviewing their information security measures.

DATA BREACH OCCURS
Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.

KEY STEPS IN RESPONDING TO A DATA BREACH

STEP 1 Contain the breach and make a preliminary assessment
- Take immediate steps to contain breach
- Designate person/team to coordinate response

STEP 2 Evaluate the risks for individuals associated with the breach
- Consider what personal information is involved
- Determine whether the context of the information is important
- Establish the cause and extent of the breach
- Identify what is the risk of harm

STEP 3 Consider breach notification
- Risk analysis on a case-by-case basis
- Not all breaches necessarily warrant notification

SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?
Where there is a real risk of serious harm, notification may enable individuals to take steps to avoid or mitigate harm. Consider:

- Legal/contractual obligations to notify
- Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities

Process of Notification
- When? - as soon as possible
- How? - direct contact preferred (mail/phone)
- Who? - entity with the direct relationship with the affected individual
- What? - description of breach, type of personal information involved, steps to help mitigate, contact details for information and assistance.

SHOULD OTHERS BE NOTIFIED?

- Office of the Australian Information Commissioner
- Police/Law Enforcement
- Professional or Regulatory Bodies
- Other agencies or organisations affected by the breach or contractually required to notify

STEP 4 Review the incident and take action to prevent future breaches
- Fully investigate the cause of the breach
- Consider developing a prevention plan
- Option of audit to ensure plan implemented
- Update security/ response plan
- Make appropriate changes to policies and procedures
- Revise staff training practices
Appendix A – APP 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.
Appendix B – Contact list: State and Territory privacy contacts

Information and Privacy Commission New South Wales

*Telephone*
(02) 8019 1600

*Post*
GPO Box 7011
Sydney NSW 2001

*Facsimile*
(02) 8114 3755

*Email*
privacyinfo@privacy.nsw.gov.au

*Website*
www.ipc.nsw.gov.au

Privacy Victoria

*Telephone*
1300 666 444 (Within Australia: local call cost, but calls from mobile and payphones may incur higher charges)

+61 3 8619 8719 (From outside Australia)

*Post*
GPO Box 5057
Melbourne Victoria 3001
Australia

*Facsimile*
Local call within Australia: 1300 666 445 (local call cost, but calls from mobile and payphones may incur higher charges)

From outside Australia: +61 3 8619 8700

*Email*
enquiries@privacy.vic.gov.au
Office of the Australian Information Commissioner

Website
www.privacy.vic.gov.au

Office of the Information Commissioner, Queensland

Telephone
(07) 3234 7373

Post
PO Box 10143
Adelaide Street
BRISBANE QLD 4000

Facsimile
(07) 3405 1122

Email
administration@oic.qld.gov.au

Website
www.oic.qld.gov.au

State Records, South Australia

Telephone
(08) 8204 8786

Post
GPO Box 2343
Adelaide SA 5001

Facsimile
(08) 8204 8777

Email
privacy@sa.gov.au

Website
Ombudsman: Western Australia

**Telephone**
(08) 9220 7555 (Western Australia)
1800 117 000 (toll free for country and interstate callers)

**Post**
Ombudsman Western Australia
PO Box Z5386
St Georges Terrace
PERTH WA 6831

**Facsimile**
(08) 9325 1107

**Email**
mail@ombudsman.wa.gov.au

**Website**
www.ombudsman.wa.gov.au


Ombudsman: Tasmania

**Telephone**
1800 001 170 (Tasmania – toll free)
1300 766 725 (Within Australia: local call cost, but calls from mobile and payphones may incur higher charges)

**Post**
GPO Box 960
HOBART 7001

**Facsimile**
(03) 6233 8966

**Email**
ombudsman@ombudsman.tas.gov.au

**Website**
www.ombudsman.tas.gov.au
Office of the Information Commissioner, Northern Territory

**Telephone**

1800 005 610 (Northern Territory – toll free)

(08) 8999 1500

**Post**

GPO Box 3750

DARWIN NT 0801

**Facsimile**

(08) 8981 3812

**Email**

infocomm@nt.gov.au

**Website**

www.infocomm.nt.gov.au

Australian Capital Territory

ACT Government agencies are subject to the Territory Privacy Principles (TPPs) in the Information Privacy Act 2014 (ACT). The TPPs came into effect on 1 September 2014. The OAIC is undertaking some of the functions of the ACT’s information privacy commissioner, including receiving voluntary data breach notifications.

The OAIC can be contacted at:

**Phone**

1300 363 992

**Email**

enquiries@oaic.gov.au

**Website**

www.oaic.gov.au