Australian Government

Office of the Australian Information Commissioner

Data breach notification

April 2012

A guide to handling personal information security breaches

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

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

ISBN 978-1-877079-70-2

Creative Commons

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

Contents

Key messages

- This guide 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 loss and from unauthorised access, use, modification or disclosure, or other misuse.
- 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 practices.
- 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 recomended 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 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

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

Privacy Act means the *Privacy Act 1988* (Cth).[1]

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

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

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, use, modification, disclosure, or other misuse.

> ***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'.

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

NPPs means the National Privacy Principles set out in Schedule 3 of the Privacy Act, which apply to organisations unless a listed exemption applies.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act and, in general, includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers and a limited range of small businesses (see ss 6D and 6E of the Privacy Act).

TFN means Tax File Number. Part III of the Privacy Act includes provisions relating to TFNs. The OAIC has issued guidelines under s 17 of the Privacy Act to regulate the use of TFNs.

1 See www.comlaw.gov.au/Series/C2004A03712.

Who should notify	
In general	**Other considerations**
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?	
In general	**Other considerations**
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 in the table 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. For example, guidance on the OAIC's website at www.oaic.gov.au and the Attorney-General's Department website at www.ag.gov.au/www/agd/agd.nsf/page/Crimeprevention_Identitysecurity.
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 step 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.[21] **With the OAIC (where 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 33. **With the relevant state or territory privacy or information regulator (where the agency or organisation is not covered by the Privacy Act).** 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 **For further guidance on notifying the OAIC, see page 32**	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 32. 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 enquiries 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.

21 The OAIC has published guidance on resolving internal complaints. Agencies may wish to review the OAIC's Information Sheet (Public Sector) 2: *A step-by-step guide to internal investigations of privacy complaints by Australian and ACT government agencies*, available at www.privacy.gov.au/materials/types/download/8814/6612. Organisations may wish to review the OAIC's Information Sheet (Private Sector) 27 - 2008: *A step-by-step guide to internal investigations of privacy complaints by organisations*, available at www.privacy.gov.au/materials/types/download/8741/6560.

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: • third party contractors or other parties who may be affected • internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or • 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 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 notification of affected individuals, OAIC and police

A small business that rents out household items keeps credit reports of rental applicants on site in hard copy. The reports have been stamped 'out of date'.

A box of the reports goes missing. The small business is unable to locate the reports and fears they have been stolen. The credit reports include the name, current or last known address and two previous addresses, driver's licence number, date of birth and employer details.

The small business believes that missing reports may have been stolen. Accordingly, the small business contacts the police.

Due to the types of information that have been lost (which, in combination, may create a serious risk of identity theft) the small business judges that the breach is serious enough to warrant notification of rental applicants and the OAIC.

The small business knows that the credit reports relate to applicants from the last two months. It decides to notify individuals who have applied for rentals during this period that information contained in their credit report may have been compromised. In the notification, the small business advises individuals to monitor their credit reports for suspicious activity, and commits to more secure storage of credit reports in the future.

To meet that commitment, the small business reviews its physical security measures. The small business implements changes to the security measures including storing reports in a locked cabinet, and ensuring that staff understand the importance of handling the reports appropriately.

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.

An example of no notification

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 pathologist know if a fax was 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[22]
- 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 returned 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.

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[23]
- whether their stored data, both in the office and when removed from the office, requires security measures such as encryption and password protection.

22 Agencies: see footnote 14 re appointing a senior executive 'information champion' to be responsible for information management and governance.

23 Agencies may wish to review the OAIC's information sheet on portable storage devices and personal information handling, available at www.privacy.gov.au/materials/types/download/9294/6867.

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 and 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	Group 2	Group 3
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.	Application information, including full name, address, contact details, and date of birth. Also includes Medicare card number, and credit card details.	Claims information, including full name, member number, contact details, and clinical information about the treatment being claimed.
Identity apparent or ascertainable?	No – the information is aggregated statistical data only.	Yes.	Yes.
Sensitivity	None.	Substantial identifying information, Medicare card number and financial details.	Substantial identifying information, as well as information about the individual's health condition.

	Group 1	Group 2	Group 3
How could the information be used?	The information is likely to be of little or no use other than for statistical purposes.	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.	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 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.	Yes – the information could be used to cause serious harm to individuals. This could include identity theft, financial fraud, and fraud against the Medicare and PBS systems. Possibly health fraud.	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?	No.	Yes, from current member list and external sources.	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 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 enquiries 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 additional resolution is required. Alternatively, the OAIC may consider that the steps taken have adequately dealt with the matter.

Reporting a breach <u>does not</u> preclude the OAIC from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or on the Commissioner's 'own motion').

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 own motion investigation powers, 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 'own motion'. The OAIC

uses risk assessment criteria to determine whether to commence an own motion 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 21). 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 or GPO Box 2999, Canberra ACT 2601
Facsimile:	02 9284 9666
Enquiries:	enquiries@oaic.gov.au
Website:	www.oaic.gov.au

Data breach response process

MAINTAIN INFORMATION SECURITY—NPP4 AND IPP4

Protect information from misuse, loss and unauthorised access, modification or disclosure.

To comply with their obligations under the NPPs and IPPs, **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.

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 – IPP 4 and NPP 4

Information Privacy Principle 4

Storage and security of personal information

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

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

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

National Privacy Principle 4

Data security

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

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

Appendix B – Contact list: State and Territory privacy contacts

New South Wales		
Privacy NSW	Telephone	(02) 8019 1600
	Post	GPO Box 7011 Sydney NSW 2001
	Facsimile	(02) 8114 3755
	Email	privacyinfo@privacy.nsw.gov.au
	Website	www.lawlink.nsw.gov.au/Lawlink/privacynsw/ll_pnsw.nsf/pages/privacy_index
Victoria		
Privacy Victoria	Telephone	1300 666 444 (within Australia: local call cost, but calls from mobile and payphones may incur higher charges) From outside Australia: +61 3 8619 8719
	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
	Website	www.privacy.vic.gov.au
Queensland		
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
South Australia		
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	www.archives.sa.gov.au/privacy/index.html

Western Australia		
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
	E-mail	mail@ombudsman.wa.gov.au
	Website	www.ombudsman.wa.gov.au
Tasmania		
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
	E-mail	ombudsman@ombudsman.tas.gov.au
	Website	www.ombudsman.tas.gov.au
Northern Territory		
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
	E-mail	infocomm@nt.gov.au
	Website	www.infocomm.nt.gov.au