



Australian Government

Office of the Privacy Commissioner

Guide to handling personal information security breaches

August 2008

Table of contents

Key Messages.....	3
Key terms used in this guide	4
1. The purpose of this guide.....	5
2. Scope of this guide	5
3. Who should use this guide?.....	6
4. What is a personal information security breach?.....	7
5. Prevent personal information security breaches	8
6. Why breach notification is good privacy practice	12
7. Four key steps in responding to a breach.....	13
STEP 1: Contain the breach and do a preliminary assessment	14
STEP 2: Evaluate the risks associated with the breach	16
STEP 3: Consider notification.....	22
STEP 4: Prevent future breaches	32
8. The Role of the Office of the Privacy Commissioner.....	37
9. Schematic guide to breach notification	40

Key Messages

- The aim of this guide is to provide general guidance on key steps and factors for agencies and organisations to consider when responding to a personal information security breach.
- Agencies and organisations have obligations to have reasonable security safeguards in place and to take reasonable steps to protect the personal information they hold from misuse, loss and from unauthorised access, modification or disclosure.
- Personal information security breaches are not limited to malicious actions, such as theft or “hacking”, but may arise from internal errors and failures to follow information handling policies, causing accidental loss or disclosure.
- In general, if there is a **real risk of serious harm** as a result of a personal information security breach, the affected individuals should be notified.
- Notification can operate as an important mitigation strategy for individuals and it promotes transparency and trust about the organisation or agency.
- There is no specific requirement in the Privacy Act to notify individuals when and if a breach has occurred.
- Notification of a breach in appropriate circumstances is consistent with good privacy practices.
- Compliance with this voluntary guide is recommended. It is not mandatory.
- The operation of this guide could inform the Government response to the Australian Law Reform Commission’s August 2008 recommendation that mandatory breach notification be introduced into law.

Key terms used in this guide

Privacy Act

Refers to 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 (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.

Personal information security breach

Has the meaning as given in section 4 of this Guide.

IPPs

The Information Privacy Principles (IPPs) set out in s14 of the Privacy Act. Australian and ACT government agencies must comply with the IPPs.

NPPs

The National Privacy Principles (NPPs) set out in Schedule 3 of the Privacy Act. In general, the NPPs apply to all businesses and non-government organisations with a turnover of more than \$3 million, all health service providers and a limited range of small businesses.¹

TFNs

Tax File Numbers. The Privacy Act includes provisions relating to TFNs in Part III. The Office has issued Guidelines under s17 of Privacy Act to regulate the use of TFNs.

¹ See sections 6D and 6E of the Privacy Act.

1. The purpose of this guide

This guide has been developed to assist agencies and organisations to respond effectively to a personal information security breach. In particular, the guide explains when an effective response to a personal information security breach might include notification of individuals affected by the breach.

The Office has developed this guide to respond to requests for advice from agencies and organisations, and in recognition of the global trends towards breach notification. Breach notification has been introduced as law in many states in the United States and is being considered by other countries including Australia. This voluntary guide has been informed by voluntary guidelines developed by the Privacy Commissioner of Canada and the Privacy Commissioner of New Zealand.²

The guidance provided is not intended to supplant the need for mandatory breach notification, in certain circumstances, to be entered into law. Such a measure has been proposed by the Australian Law Reform Commission in August 2008.

2. Scope of this guide

Breach notification is one particular option in responding to a personal information security breach. However a key challenge is to determine in what circumstances it is an appropriate response. While establishing appropriate thresholds for requiring breach notification can be considered good privacy practice, the steps and actions outlined in the guide are not specifically required under the *Privacy Act 1988* (the Privacy Act). Therefore, compliance with this guide is voluntary.

The aim of this guide is to provide general guidance on key steps and factors for agencies and organisations to consider when responding to a personal information security breach, without the sole focus being notification of breaches.

The guide encourages a risk-analysis approach so that agencies and organisations evaluate a breach 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.

The guide also highlights the importance of preventative measures as part of a holistic information security plan.

² See Office of the Privacy Commissioner of Canada, 'Key Steps for Organisations in Responding to Privacy Breaches' (August 2007), available at http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp. and New Zealand Office of the Privacy Commissioner draft privacy breach guidelines, available at <http://www.privacy.org.nz/privacy-breach-guidelines-2/>.

It is important to note that, while the guidance is not mandatory and is of an advisory nature only, agencies and organisations do have binding legal obligations under the Privacy Act to secure personal information, as set out in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs).

It is not intended that the advice in this guide be limited to personal information security breaches that are breaches of IPP4 or NPP4³. Rather, the guide is intended to extend to any situation where personal information has been compromised.

3. Who should use this guide?

This guide has been developed for use by Australian and ACT Government agencies and private sector 'organisations'⁴ that handle personal information. As well as businesses, organisations in the not-for-profit, community and charity sectors may find the guide useful.

The guide may also be useful to small businesses that have obligations under Privacy Act, including those small businesses that may only be covered by the NPPs in respect of some of their activities⁵ or are covered by the credit reporting provisions of Part IIIA of the Privacy Act.

Government agencies of the states and the Northern Territory, as well as private sector businesses not covered by the Privacy Act, may find the guide helpful in outlining good privacy practice. However, the Privacy Commissioner would not have a role in receiving notifications about personal information security breaches from these entities.

State and Northern Territory government agencies should also consider the role of relevant Privacy or Information Commissioners in their own jurisdictions.

³ IPP4 and NPP4, require agencies and organisations, respectively, to protect information they hold from misuse and loss and from unauthorised access, modification or disclosure.

⁴ An organisation, as defined under the Privacy Act 1988, is

- (a) an individual, or;
- (b) a body corporate or;
- (c) a partnership or;
- (d) any other unincorporated association or;
- (e) a trust;

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality.

⁵ For example, organisations that are reporting entities for the purposes of the *Anti Money Laundering and Counter Terrorism Financing Act 2006* are required to comply with the NPPs in terms of these activities, even if they are otherwise exempt under the Privacy Act.

4. What is a personal information security breach?

A personal information security breach occurs when personal information is subject to loss or unauthorised access, use, disclosure, copying or modification.

The use of the term 'personal information security' breach is consistent with the Privacy Act, which regulates the handling of personal information. This term is used in preference to the term 'data' which is generally not used in the Privacy Act.⁶

Personal information security breaches can occur in a number of ways. Some of the most common breaches happen when personal information held by an agency or organisation is lost, misused, mistakenly disclosed or stolen. Some examples include:

- lost or stolen laptops, removable storage devices, or physical files containing personal information
- paper records inadequately recycled or left in garbage
- computer hard drives and other storage media being disposed of without erasing contents
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organisation and
- employees accessing personal information outside the requirements of their employment.

It is important to recognise that personal information security breaches are not limited to external malicious actions, such as theft or 'hacking', but may just as often involve internal errors and failures to follow established information handling procedures. While there may be no harm intended, these types of breach can affect individuals' privacy as much as malicious actions.

⁶ Although the titles for NPP 3, NPP 4 and NPP 9 all refer to 'data' (being the 'Data quality', 'Data security' and 'Transborder data flows' principles respectively), this term tends not to be used in the substantive provisions of the Act. See *Privacy Act 1988* (Cth), Schedule 3. The NPPs are available at <http://www.privacy.gov.au/publications/npps01.html>.

5. Prevent personal information security breaches

Security is a basic element of information privacy.⁷ In Australia, this principle is reflected in the Privacy Act in both the IPPs and the NPPs.

5.1 Obligations under the Privacy Act

The IPPs regulate the way most Australian and ACT Government agencies handle personal information. These principles cover the collection, storage, use, disclosure and access obligations of those agencies.

The NPPs regulate the way private sector organisations handle personal information. These principles cover collection, storage, use, disclosure and access obligations of organisations covered by the Privacy Act. In general the NPPs apply to all businesses and non government organisations with a turnover of more than \$3 million, all health service providers and a limited range of small businesses.⁸

Agencies and organisations are required to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. This requirement is set out in IPP 4 for public sector agencies and NPP 4 for private sector organisations.⁹ (See Appendix A for IPP4 and NPP4.)

Section 18G(b) of the Privacy Act imposes equivalent obligations on credit reporting agencies and all credit providers. Similarly, guideline 6.1 of the statutory guidelines regulating Tax File Numbers (TFN) requires TFN recipients to afford TFNs security safeguards as are reasonable in the circumstances.

⁷ 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

http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

The *Privacy Act 1988* (Cth) was enacted to implement the OECD guidelines in Australia, as recognised in the preamble to the Act.

⁸ For further information on coverage of the NPPs, see Information Sheet 12–2001 *Coverage of and Exemptions from the Private Sector Provisions*, available at http://www.privacy.gov.au/publications/IS12_01.html.

⁹ The Office has provided further guidance on compliance with the information security principles elsewhere, available at

Guidelines to the Information Privacy Principles (principles 4–7) (for Australian and ACT Government agencies), available at

<http://www.privacy.gov.au/government/guidelines/index.html>.

Guidelines to the National Privacy Principles (for private sector organisations), available at

http://www.privacy.gov.au/publications/nppgl_01.html.

Information Sheet 6–2001: Security and personal information

Provides information for organisations on compliance with NPP 4 available at

http://www.privacy.gov.au/publications/IS6_01.html.

5.2 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.¹⁰ These other requirements can include the Australian Government's *Protective Security Manual* and the *Information and Communications Technology Security Manual* (also known as ACSI 33).

Organisations may also be subject to additional obligations through sectoral specific-legislation in respect of particular information they hold. For example, Part 13 of the *Telecommunications Act 1997* (Cth) 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 confidentiality of particular information.

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

5.3 Considerations for keeping information secure

While the focus of this guide is the process of responding to a personal information security breach agencies and organisations should aim to avoid such breaches in the first place by ensuring that they have appropriate security safeguards in place consistent with IPP4 or NPP4.

Some of the information in Step 4 of the guide (see page 32) could equally be used by agencies or organisations as a way of assessing what security measures they should have in place to avoid a breach occurring.

What are reasonable steps to secure personal information will depend on context, including:

- the sensitivity to the individual of the personal information the organisation holds
- the harm that is likely to result to people if there is a breach of their personal information
- the potential for harm (reputational or other damage) to the agency or organisation if the personal information in question were breached
- how the agency or organisation stores, processes and transmits the personal information (for example, paper-based or electronic records, or 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

¹⁰ See the Office's *Guidelines to the Information Privacy Principles (principles 4–7)* for a brief overview of existing guidance on security standards for agencies, available at <http://www.privacy.gov.au/government/guidelines/index.html>.

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
- **policy development** – developing a policy or range of policies that implements 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 personal information security breaches. This position could have responsibility for establishing policy and procedures, training staff, co-ordinating reviews and audits and investigating and responding 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.
- **monitor 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
- **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
- **audits** – undertaking regular audits to detect system weaknesses and/or breaches and
- **appropriate contract management** – conducting appropriate due diligence where services are contracted, particularly in terms of the IT security policies and practices that the service provider has in place and then monitoring compliance to these policies through periodic audits.

Further, in seeking to prevent personal information security breaches, agencies and organisations should consider their other privacy obligations under the IPPs and NPPs. 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:

- **What personal information is necessary to be collected?** Simply put, personal information that is never collected, cannot be mishandled and therefore the risk of mishandling is avoided. Both IPP 1 and NPP 1 require

that agencies and organisations, respectively, only collect personal information that is necessary for one or more of their functions or activities. IPP 3 also requires that a collector of personal information take steps to ensure that the information collected is relevant to the purpose for which it was collected.

- **How long does the personal information need to be kept?** NPP 4.2 requires organisations to securely destroy or permanently de-identify information that is no longer needed for the permitted purposes for which it may be used or disclosed. Although the IPPs do not contain a similar obligation, agencies should nevertheless consider retention practices, subject to other applicable record-keeping requirements such as those contained in the Commonwealth Archives Act.

6. Why breach notification is good privacy practice

Both the IPPs and the NPPs require that personal information be held securely. Failure to comply constitutes an interference with privacy under the Privacy Act.

However, the Privacy Act does not expressly require an agency or organisation to notify individuals if personal information is subject to a breach of information security safeguards. In addition, breaches of personal information may arise from activity that is not regulated by the Privacy Act, such as acts and practices relating to employee records held by private sector organisations.¹¹

Notifying individuals where a breach affects their personal information is consistent with good privacy, for these reasons:

- **Notification as a reasonable security safeguard:** As part of the obligation to keep personal information secure, notification may in some circumstances be considered as a reasonable step in the protection of personal information against misuse, loss or unauthorised access, modification or disclosure.
- **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.¹² 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.
- **Notification as restoring control over personal information:** Privacy is valued, not only because it underpins our human dignity but also because it gives individuals a measure of control in their everyday interactions as to how personal information about them is handled. To this end, the Privacy Act seeks to ensure that individuals know why information is collected, what it is used for, who it is ordinarily disclosed to and provides for rights of access and correction.

Notification of a breach in appropriate circumstances is consistent with good privacy practices and is to be encouraged in maintaining a community in which privacy is valued and respected.

¹¹ Employee Records (as defined in s6 of the Privacy Act) directly related to an employment relationship of current or former employees are exempt from coverage by the NPPs under s7B(3).

¹² See the 'openness 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 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. This principle is reflected in NPP 5 and IPP 2 in the *Privacy Act 1988* (Cth).

7. Four key steps in responding to a breach

Personal information security breaches can be caused 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.

Given this context, it is clear that there is no single way of responding to a personal information security 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.

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

- Step 1: Contain the breach and do a preliminary assessment**
- Step 2: Evaluate the risks associated with the breach**
- Step 3: Consider notification**
- Step 4: Prevent future breaches**

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

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 and organisation has discovered or suspects that a personal information security breach has occurred, they should take immediate common sense steps to limit the breach. These may include

Contain the Breach	<p>Take whatever steps possible to immediately contain the breach.</p> <p>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 correct weaknesses in physical or electronic security.</p> <p>Assess whether steps can be taken to mitigate the harm an individual will suffer as a result of a breach.</p> <p>For example, if its 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?</p>
Initiate a preliminary assessment	<p>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.</p> <p>Determine the need to assemble a team that could include representatives from appropriate parts of the agency or organisation.</p>
Does anyone need to be notified immediately?	<p>Determine who needs to be made aware of the breach internally, and potentially externally, at this preliminary stage.</p> <p>In some cases it may be appropriate to notify individuals immediately.</p> <p>Escalate the matter internally as appropriate, including informing the person within the agency or organisation responsible for privacy compliance.</p> <p>It may also be appropriate to report such breaches to relevant internal investigations units.</p> <p>If the breach appears to involve theft or other criminal activity, notification to police should generally occur.</p>

Other matters	<p>Be careful not to compromise the ability of law enforcement agencies to investigate the breach, for example, by making details of the breach public too early.</p> <p>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, and ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.</p>
----------------------	--

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.

A jobseeker whose résumé is on the site forwards the recruitment agency an email she received 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 she has to do to secure the job is to provide her bank accounts details so she can be paid.

While 'phishing' is common on the internet, 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 seeks 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 site 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 to the individual associated with the breach.

Consider the following factors in assessing the risks:

- (a) What personal information is involved
- (b) What is the context of the information
- (c) Establish the cause and extent of the breach
- (d) Asses what is the risk of harm that could result to individuals
- (e) Identify what other harms or risks could arise

(a) Consider what personal information is involved	
Considerations	Comments and examples
Does the type of information create a greater risk of harm?	<p>Some information is more likely to cause an individual harm if it is compromised, whether that harm is physical, financial or psychological. For example, health information, government-issued identifiers such as Medicare numbers, driver licence and health care numbers, 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.</p> <p>Also, a combination of personal information typically creates a great risk of harm than a single piece of personal information.</p> <p>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'.</p> <p>The permanence of the information may be more significant if it is protected by encryption – overtime, 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 an algorithm is broken.</p>
Who is affected by the breach?	<p>Employees, contractors, the public, clients, service providers, other agencies or organisations?</p> <p>Remember that certain people may be particularly at risk of harm. A personal information security breach involving name and address of a person might not always be considered high risk. 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. The risk may be less if the breach relates to businesses that service the refuge.</p>

(b) Determine the context of the affected information	
Considerations	Comments and examples
<p>What is the context of the personal information involved?</p>	<p>For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive.</p> <p>While publicly available information such as that found in a public telephone directory may be less sensitive, this 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?</p> <p>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.</p>
<p>Have there been other breaches that could have a cumulative effect?</p>	<p>A number of small, seemingly insignificant, breaches could have an accumulative 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 accumulative affect of the breaches is considered.</p> <p>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.</p>
<p>How could the personal information be used?</p>	<p>Could the information be used for fraudulent or otherwise harmful purposes, such as to significantly embarrassing the individual?</p> <p>Could the affected information be easily combined either with each other or with readily publicly available information to create a greater risk of harm to the individual?</p>
(c) Establish the cause and extent of the breach	
Considerations	Comments and examples
<p>Is there a risk of ongoing breaches or further exposure of the information?</p>	<p>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?</p>
<p>Is there evidence of theft?</p>	<p>Is there evidence that suggests theft, and was the information the target? For example where a laptop is stolen can it be determined whether it was the information on the laptop or the laptop itself that the thief wanted?</p> <p>Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as possible law enforcement.</p>

<p>Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?</p>	<p>Is the information rendered unreadable by security measures in place to protect the stored information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?</p> <p>For example, if a laptop containing adequately encrypted information is stolen, subsequently recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.</p>
<p>What was the source of the breach?</p>	<p>For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does it seem to have been lost or misplaced?</p> <p>The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.</p> <p>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 opened a client's record to browse the record, or to use or disclose that information without a legitimate business reason for doing so.</p>
<p>Has the personal information been recovered?</p>	<p>For example, has a lost laptop been found or returned? If the information has been recovered, are there any signs that it has been tampered with?</p>
<p>What steps have already been taken to mitigate the harm?</p>	<p>Have the agency or organisation contained the breach so that its full extent can be assessed? Are further steps required?</p>
<p>Is this a systemic problem or an isolated incident?</p>	<p>When checking the source of the breach, it is important to check whether any similar breaches could 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 risk posed.</p>

<p>How many individuals' are affected by the breach?</p>	<p>If the breach is a result of a systemic problem, there may be more people affected than first anticipated.</p> <p>Even where the breach involves accidental and unintentional misuse of information; if the breach affects many individuals then this may create greater risks that the information will be misused. The agency or organisation's response should be proportionate.</p> <p>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.</p>
<p>(d) Assess what is the risk of harm that could result to individuals</p>	
<p>Considerations</p>	<p>Comments and examples</p>
<p>Who is the recipient of the information?</p>	<p>Is there likely to be any relationship between the unauthorised recipients and the affected individuals?</p> <p>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? Or was the disclosure to a party to which the individual would object or is the subject of a restraining order. Or to co-workers who have no need to have this information?</p> <p>Or was the recipient a trusted, known entity or person that would reasonably be expected to return 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.</p>
<p>What harm to individuals could result from the breach?</p>	<p>Examples include:</p> <ul style="list-style-type: none"> • threat to physical safety • identity theft • threat to emotional wellbeing • financial loss • loss of business or employment opportunities or • humiliation, damage to reputation or relationships • workplace or social bullying or marginalisation.
<p>(e) Identify what other harms or risks could arise</p>	
<p>Other possible harms</p>	<p>Examples include:</p> <ul style="list-style-type: none"> • loss of trust in the agency or organisation • loss of assets • financial exposure • regulatory penalties • extortion • reputational damage • legal proceedings. • risks to national security • impact on secrecy and access provision

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 safely 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 Privacy Commissioner, particularly as there is a real possibility that individuals may complain about the breach.

State government agency discovers routine breaches

A state government agency undertakes a periodic audit of user access records. The audit reveals an unusual pattern of client account enquiries in one department of the agency. The client records being browsed belong to well known celebrities and contain address information, along with other details. The unauthorised viewing has occurred over a 12 month period.

After making further enquiries which included interviewing the relevant staff, department staff, managers and later the department head, it is determined that the staff were intentionally browsing client records without any legitimate business purpose. There is no evidence that this information has been disclosed to any third party.

However, the agency recognises that the address details may be information that is not readily available elsewhere, as many of the individuals are unlikely to have their addresses in other public sources.

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

As a state government agency, the jurisdiction of the Privacy Act does not apply. There is likely to be little purpose in notifying the Privacy Commissioner. However, in this case, the state does have its own privacy law and regulator. The state government agency seeks advice from its own regulator as to whether notification is required.

STEP 3: Consider notification

Notification can be an important mitigation strategy that has the potential to benefit both the agency or organisation and the individuals affected by a personal information security breach. The challenge is to determine when notification is appropriate. While notification is an important mitigation strategy, it will not always be the appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitise 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 personal information security breach creates a real risk of serious harm to the individual, those affected 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
- consider whether it is appropriate to inform other third parties about the personal information security breach such as the police, professional bodies, the Privacy Commissioner or other regulators or professional bodies.

(a) Deciding whether to notify affected individuals

In notifying affected individuals, a key consideration is whether notification is necessary in order to avoid or mitigate serious harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed.

Agencies and organisations should consider the following factors when deciding whether to notify:

- 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 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 very 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?

- What are the consequences of failing to notify affected individuals? If individuals subsequently find out about the breach through the media for example, what could be the associated loss of trust that the agency or organisation sustains?

(b) Process of notification

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

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

When to notify:	
In general	Other considerations
Notification of individuals affected by the breach should occur as soon as reasonably possible.	<p>If law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.</p> <p>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.</p>
How to notify:	
In general	Other considerations
<p>The preferred method of notification is direct either by phone, letter, email or in person – to affected individuals.</p> <p>Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known.</p>	<p>Preferably notification should ‘stand-alone’ 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.</p> <p>Using multiple methods of notification in certain cases may be appropriate.</p> <p>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 computer if it would not otherwise be apparent.</p> <p>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.</p>

Who should notify:	
In general	Other considerations
<p>Typically, the agency or organisation that has a direct relationship with the customer, client or employee should notify the affected individuals.</p> <p>This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate.</p>	<p>Joint and third party relationships can raise complex issues – 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).</p> <p>Each situation will vary and organisations and agencies will have to consider what is best on a case by case basis. However some relevant considerations might be:</p> <ul style="list-style-type: none"> • Where did the breach occur? • Who does the individual identify as their “relationship” manager? • Does the agency or organisation have contact details for the 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 organisation’s or agency’s activities?
Who should be notified?	
In general	Other Considerations
<p>Generally it should be the individual/s who are affected. However, in some cases it may be appropriate to notify the individual’s guardian or authorised representative on their behalf.</p>	<p>There may be circumstances where carers or authorised representatives should be notified as well as, or instead of, the individual.</p> <p>Where appropriate, clinical judgement may be required where notification may exacerbate health conditions, such as acute paranoia.</p>

(c) What should be included in the notification?

The content of notifications will vary depending on the particular breach and the method of notification chosen. 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 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. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a government issued identification number, personal health card or driver 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 Office of the Privacy Commissioner's website www.privacy.gov.au and the Attorney-General's Department website at http://www.ag.gov.au/www/agd/agd.nsf/page/Crimeprevention_Identitysecurity
Agency/ Organisation contact details	Contact information of areas 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 should they have further questions.
Whether breach notified to regulator or other external contact(s)	Indicate whether the agency or organisation has notified the Office of the Privacy Commissioner or other parties listed in the table 4(d).
Legal implications	The precise wording of the notice may have legal implications, so should be checked accordingly. This could include secrecy obligations that apply to agencies.

How individuals can lodge a complaint	<p>With the agency or organisation</p> <p>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.</p> <p>With the Privacy Commissioner</p> <p>Explain that if individuals are not satisfied with the response by the agency or organisation resolve the issue, that they can make a complaint to the Office of the Privacy Commissioner.</p> <p>Include the contact information for the Office of the Privacy Commissioner:</p> <p>Telephone 1300 363 992 (local call cost, but calls from mobile and payphones may incur higher charges)</p> <p>TTY 1800 620 241 (this number is dedicated for the hearing impaired only, no voice calls)</p> <p>Post GPO Box 5218 Sydney NSW 2001</p> <p>Facsimile +61 2 9284 9666</p> <p>E-mail privacy@privacy.gov.au</p> <p>Website www.privacy.gov.au</p>
--	--

(d) Others to Contact

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

<p>Privacy Commissioner</p>	<p>Agencies and organisations may decide to report significant personal information security breaches to the Privacy Commissioner. The potential benefits of notifying the Privacy Commissioner, together with what the Privacy Commissioner can and cannot do about a notification, are set out in Section 8 of this guide.</p> <p>The following factors should be considered in deciding whether to report a breach to the Privacy Commissioner:</p> <ul style="list-style-type: none"> • 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 individuals affected have been notified and • if there is a reasonable expectation that the Office may receive complaints or inquiries about the breach.
<p>Police</p>	<p>If theft or other crime is suspected.</p> <p>The Australian Federal Police should also be contacted if a compromise to national security is suspected.</p>
<p>Insurers or others</p>	<p>If required by contractual obligations.</p>
<p>Credit card companies, financial institutions or credit reporting agencies</p>	<p>If their assistance is necessary for contacting individuals or assisting with mitigating harm.</p>
<p>Professional or other regulatory bodies</p>	<p>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, the Australian Communications and Media Authority and the Australian Prudential Regulatory Authority have their own requirements in the event of a breach.</p>

<p>Other internal or external parties not already notified</p>	<p>Agencies and organisations should consider the potential impact that the breach and notification to individuals may have on third parties and take actions accordingly. For example, third parties may be affected if individuals cancel their credit cards or if financial institutions issue new cards.</p> <p>Consider:</p> <ul style="list-style-type: none"> • third party contractors or other parties who may be impacted; • internal business units not previously advised of the breach, (e.g. communications and media relations, senior management); or • union or other employee representatives
<p>Agencies that have a direct relationship with the information lost / stolen</p>	<p>Agencies and organisations should consider whether an incident compromises Commonwealth agency identifiers such as Tax File Numbers (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.</p>

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 and the Bank then contacts Diego to notify him about what has occurred.

The bank contacts Diego by phone to notify him about 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 occurring again. 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 undertakes an investigation of the matter which includes getting reports from the mailing house it uses to generate and despatch customer correspondence. While the mailing house had 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 also reviews the compliance measures 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 Privacy Commissioner

A memory stick containing the employee records of 200 employees of a Commonwealth 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. Information 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 existence 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 Privacy Commissioner of the breach and explains what steps it is taking to resolve the situation.

A senior staff member emails staff to notify them of the breach. In the notification she offers staff an apology for the breach, explains what types of information were breached, notes that the Privacy Commissioner 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. In the notification to staff, the senior staff member also provides staff with details about how they can have a new TFN issued and informs staff that if they are unhappy with the steps the agency has taken they can make a complaint to the Office of the Privacy Commissioner.

An example of notification of affected individuals, Privacy Commissioner and police

A ticket retailer sells concert tickets at various outlets and online. Online purchases are done on a secure site using a credit card. During a routine security check, the ticket retailer discovers through the use of intrusion detection software that the database connected to its secure site has been compromised and customer information stolen. The ticket retailer takes steps to contain the breach and then, based on its belief that criminal activity has been involved, contacts the police.

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

Once satisfied that notification will not compromise police investigations, the retailer notifies the Privacy Commissioner of the breach and then emails affected ticket purchasers. In notifying the ticket purchasers, the retailer explains exactly what happened and when; that the police have been investigating; and that the Privacy Commissioner has been notified. It also suggests that affected ticket purchasers monitor their credit card accounts and contact their financial institution if they have any concerns.

An example of notification of affected individuals, Privacy Commissioner and police

A small business that rents out household items keeps credit reports of rental applicants on site in hard copy. These 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, drivers licence number, date of birth and employer details.

Based on the belief that theft may be involved, the small business alerts 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 Privacy Commissioner.

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 the commitment to store reports more securely, the small business undertakes to review physical security measures, including by storing reports in a locked cabinet and ensures that staff understand the importance of handling the reports appropriately.

An example of no notification

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

Despite the assistance of the transport authority, the Department is unable to locate the memory stick. Following a preliminary assessment of the breach, the Department undertakes to evaluate the risks associated with the loss of the memory stick.

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

Further evaluation of the risks associated with the loss of the memory stick reveal 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 the IT team, decides that notification of individuals whose personal information was held on the memory stick is not necessary.

An example of no notification

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

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

The pathologist recognises that the GP is bound by ethical duties and is familiar with principles of confidentiality and privacy. Accordingly, the pathologist is confident that Dr Angel 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 individual.

The pathologist decides not to notify but does review his practices to avoid a similar breach occurring in the future. To reduce the chance of such mistakes happening again, the specialist puts in place a series of steps, including ensuring that administrative staff are counselled to exercise care in checking that fax numbers are accurate. The specialist also considers taking the step of routinely phoning recipients to put them on notice 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, and may allow the intended recipient to let the sender know if it is 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 of the breach and consider whether to either evaluate the existing prevention plan or develop one.

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

This plan may include the following:

- 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 regularly 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 (e.g. dealers and retailers).

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.

Some suggestions for being prepared to respond to a breach are:

- 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 from the breach.

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

- Depending on the size of the agency or organisation, a management group responsible for responding to personal information breaches could be established, with representatives from relevant areas that may be needed to investigate an incident, conduct risk assessments and make appropriate decisions (e.g. privacy, senior management, IT, public affairs, legal).

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

- Include information in the agency or organisation's privacy policy about how it respond to breaches. This could include letting individuals know 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 asking recipients to verify their account details, passwords and other personal information.

Tips for preventing future breaches

Some of the measures that have resulted from real-life personal information security breaches are:

- the creation of a senior position in the agency or organisation with specific responsibility for data security
- 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
- ensure hard drives and other storage media are erased before being disposed
- use secure couriers and appropriate tamper proof packaging in the transport of bulk data and
- a ban on the removal of unencrypted laptops and other portable devices from government buildings.

Technological advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of personal information security 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 disks, USB storage devices, laptops and other portable devices or in physical files and
- whether their stored data, both in the office and when removed from the office, requires encryption security.

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 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 over 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 onto 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 is 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.	Claim 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.

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. 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, accidental loss. But theft is also a possibility. As the source is unclear, and given the sensitivity of much of the information, insurers decide to assume a worst case scenario.		
Severity	Information was not encrypted or recovered. The large number of records involved and the sensitivity of the much 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.
<p>The evaluation shows that a real risk of serious harm arises for Group 2 and 3 individuals and that the information in Group 1 is not personal information.</p> <p>Step 3 – Consider Notification</p> <p>The evaluation indicates that individuals in Groups 2 and 3 should be notified about the breach, about 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 report. 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.</p>			

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 for individuals in Group 2 tells them that the information they provided on their application form may have been compromised, including their Medicare number and credit card details. 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 Office of the Privacy Commissioner, and suggests 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 will be 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.

While the insurer does not have to notify the Privacy Commissioner, it decides to do so given the large number of individuals affected and sensitive nature of the information. It explains to the Privacy Commissioner what steps it has taken to address the breach.

Step 4 – Preventing Future Breaches

Once immediate steps have been taken to respond to the breach, the Chief Information Officer 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.

8. The Role of the Office of the Privacy Commissioner

The Office, on behalf of the Privacy Commissioner, has the function of investigating possible breaches of the Privacy Act. It also has the function of providing advice to agencies and organisations on any matter relevant to the operation of the Privacy Act. While the Office has no formal role in relation to breach notification, it may provide general advice on how to respond to a personal information security breach.

Step 3(d) of the guide provides guidance on when it may be appropriate to notify the Office of a personal information breach. Consistent with its statutory functions, the Office may consider whether it needs to investigate the conduct.

A personal information breach may constitute a breach of information security obligations under the IPPs or NPPs, and in that circumstance it will be an interference with an individual's privacy.¹³ However, the Office cannot make a decision on whether there has been a breach of the Act until it has conducted an investigation.

If an individual thinks an agency or organisation 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 Privacy Commissioner. The Office may investigate and may attempt to resolve the matter by conciliation between the parties.

The Privacy Act does not specify penalties for breaches of the IPPs or NPPs, though deliberate contravention of some of the credit reporting provisions in Part IIIA of the Privacy Act does carry penalties. The Privacy Commissioner may make determinations requiring the payment of compensation for damages or other remedies, such as the provision of access or the issuance of an apology. These determinations can be enforced by the Federal Court or Federal Magistrates Court.

The Office also has the power to initiate an investigation on its own motion in appropriate circumstances without first receiving a complaint.

Agencies should also be aware that, under s 27(1)(j) of the Privacy Act, the Privacy Commissioner can inform the Cabinet Secretary, as the Minister responsible for the Privacy Act, of action that needs to be taken by an agency in order to achieve compliance by the agency with the IPPs.

The Office conducts its investigations in private, and in general will not publicise details of its inquiries. However, consistent with its roles of education and enforcement, in some circumstances the Commissioner may publicise information about the information management practices of an agency or organisation.

¹³ See sections 13 (agencies) and 13A (organisations) of the *Privacy Act 1988* (Cth).

8.1 Reporting a personal information security breach to the Office

The Privacy Act does not specifically require agencies and organisations to report personal information security breaches to the Privacy Commissioner. However, agencies and organisations may choose to notify the Office of a personal information security breach where the circumstances indicate that it is appropriate to do so, as set out in Step 3(d). The following are some potential benefits from notifying the Office of a personal information security breach:

- An agency or organisation's decision to notify the Office on its own initiative may be viewed by the public as a positive action. It tells clients and the public that the agency or organisation views the protection of personal information as an important and serious matter. This may enhance public/client confidence in the agency or organisation.
- It can assist the Office 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 provide the Office with details of the matter, and the action taken to address it, and prevent future occurrences, then it may be that any complaints received can be dealt with more quickly based on that information. 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, or alternatively, the Office may consider that the steps taken have adequately dealt with the matter.

It is important to note that reporting a breach does not preclude the Office from receiving complaints and conducting an investigation of the incident (whether in response to a complaint or of its own motion).

If the agency or organisation decide to report a personal information security breach to the Office, the following provides an indication of what the Office can and can't do:

What the Office can do:

- Provide general information about obligations under the Privacy Act, factors to consider in responding to a personal information security breach and steps to take to prevent similar future incidents.
- Respond to community enquiries about the breach and explain possible steps individuals can take to protect their personal information.

What the Office 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 Office) if the Office is notified of a breach.

When the Office receives a complaint about an alleged breach of the Act, in most cases, the Office must investigate. As set out above, the Office may also investigate an act or practice in the absence of a complaint, on its 'own motion'. The Office uses risk assessment criteria to determine whether to investigate a matter on its own motion. These 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, are investigating.

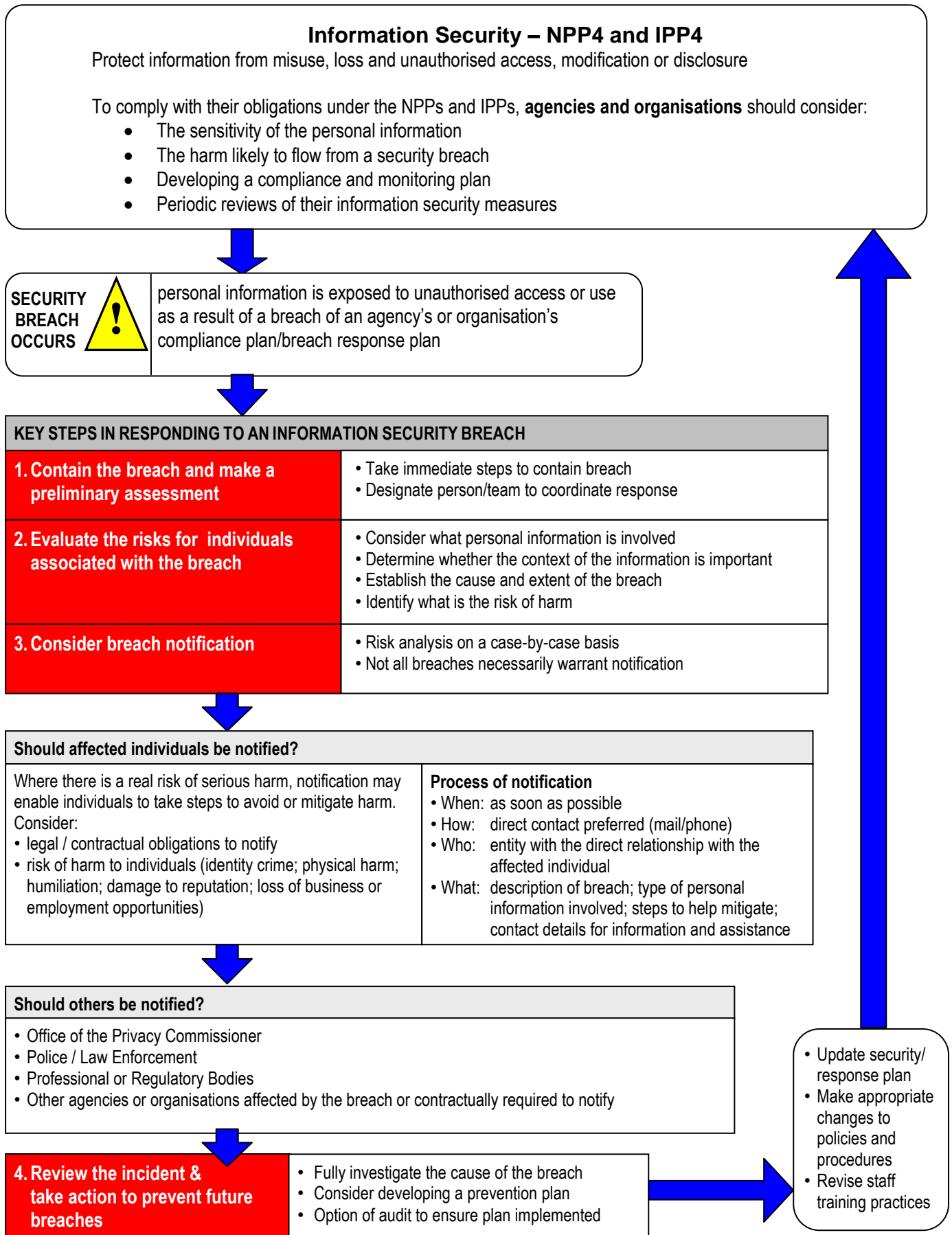
These factors are similar to those included in the risk assessment criteria for responding to a personal information security breach.

8.2 What to put in a notification to the Office

Any notice provided to the Office should contain similar content to that provided to individuals. It should not include personal information about the affected individuals. It may be appropriate to tell the Office:

- a description of the breach
- the type of personal information
- what response the agency or organisation has made to the breach
- what assistance has been offered to affected individuals
- who is the contact person
- whether the breach notified has to other external contact(s).

9. Schematic guide to breach notification



Appendix A

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.

Web HTML, Word and PDF published August 2008
ISBN 978-1-877079-62-7
© Commonwealth of Australia 2008