STATE RECORDS
of South Australia

Personal Information Breach Guideline

Introduction

Personal information is increasingly vulnerable as technology advances. Agencies who are required to manage that information are responsible for managing the risks of inappropriate exposure. Financial fraud, identity theft and harm to a person are all potential consequences of mismanagement of personal information.

Notifying individuals whose information has become exposed promotes an open and transparent government, assists in maintaining public trust in government services and enables individuals and organisations to exercise control over their information, privacy and security. It shows a willingness to assist with implementing the precautions necessary to mitigate the risks associated with exposed personal information. This assistance ensures the public are confident that government agencies respect their personal information.

Managing breaches can be complex. Agencies may wish to seek legal advice for assistance.

Purpose

This Guideline has been developed to provide advice to South Australian government agencies about how to manage breaches of personal information.

For the purposes of this Guideline, a 'Breach' occurs when personal information which is held by a government agency or a contracted service provider and is not publicly available, is lost or subjected to unauthorised access or disclosure.

The Guideline advises on the prompt action agencies should take where a breach has been identified.

Guideline

What is personal information?

Personal information is information or an opinion, whether true or not, relating to a natural person, or the affairs of a natural person, whose identify is apparent, or can reasonably be ascertained, from the information or opinion[1]. A natural person in this context is a living human being.

Personal information can include names, address, date of birth, financial or health details, ethnicity, gender, religion, allegations of criminal activity etc. The personal information held by an agency may be collected in paper form, verbally or through electronic or analogue means.

[1] PC012 Information Privacy Principles Instruction

In delivering government services to the community, agencies collect and manage large amounts of personal information.

Personal information is considered an official record as defined by section 3(1) of the *State Records Act 1997*. This includes information, data and records, in any format (digital, hardcopy or analogue), where it is created or received through the conduct of government business (including handling of information by a contracted service provider[2]).

How is personal information collected, stored, managed and used?

The collection, storage, use and disclosure of personal information by South Australian government agencies is governed by the Department of the Premier and Cabinet (DPC) Circular: PC012 Information Privacy Principles Instruction (IPPI).

Oversight of these principles is the responsibility of the principal officer (usually the Chief Executive) of the agency, with advice from the Privacy Committee of South Australia (the Privacy Committee).

Other governing frameworks

There are several governing frameworks in the South Australian government relating to the safety and security of personal information. This Guideline is not meant to override any other framework or duplicate processes and reporting requirements; instead, it should align and complement.

For example, the South Australian Protective Security Framework (SAPSF) and the South Australian Cyber Security Framework (SACSF) provide protective security policy and guidance for South Australian government agencies. This Guideline is designed to work alongside both security frameworks.

South Australian public sector employees are bound by the Code of Ethics. The Code has some confidentiality obligations that all employees must abide by.

The South Australian *Public Sector (Data Sharing) Act 2016* provides boundaries around specific uses of the personal information collected, used and held by agencies.

The Information Sharing Guidelines give providers of services to children, young people and adults, confidence in sharing information when required to prevent harm or respond to current threats to safety and wellbeing.

There is also legislation which may apply to specific agencies around the collection, storage, use and disclosure of information, for example the *Health Care Act 2008,* the *Mental Health Act 2009,* the *Motor Vehicles Act 1959* and the *Education and Children's Services Act 2019* to name a few.

The Commonwealth *Privacy Act 1988* does not generally apply to South Australian government agencies. However, the Commonwealth Act requires agencies that hold tax file number (TFN) information, to comply with the Commonwealth's Notifiable Data Breaches scheme, but only in respect to TFN information. For further information relating to breaches involving TFN information, refer to Attachment 4.

[2] Contracting-and-Information-Assets-Standard-V1.3.pdf

How do personal information Breaches occur?

Breaches can occur in several ways, such as:

- human error (accidental)
- procedural or internal error
- system error (malfunction)
- malicious or criminal attack (deliberate disclosure, theft of physical assets or the theft or misuse of electronic information, e.g. a cyber-attack).

How can affected parties of a personal information Breach be impacted?

Breaches have the potential to result in real harm to an individual or an agency, or both.

Outcomes can vary depending on the type and seriousness of the Breach, what type of personal information was exposed, and how much. All can result in life changing situations such as:

- identity theft
- financial loss
- threat to physical safety or emotional wellbeing
- loss of business or employment opportunities
- damage to reputation or relationships
- bullying or marginalisation

If not contained, Breaches can lead to the sourcing of other publicly available information (e.g. social media data) for identity theft or financial fraud.

How should agencies manage personal information Breaches?

When a Breach occurs, prompt action must be taken to:

1. contain the Breach, if possible
2. identify the risks
3. report the Breach to the relevant authorities
4. notify affected parties, and
5. implement remedial action and review.

1. Contain the Breach

After confirming the Breach has occurred, where possible, steps must be taken to contain the Breach immediately to prevent the personal information being further compromised. The steps to contain the Breach will depend on the nature of the Breach.

Some common actions include:

- stopping unauthorised practice
- stopping employee access
- recovering the records
- shutting down the system that was breached
- changing device and system access codes, and
- correcting weaknesses in physical or electronic security.

2. Identify the risks

Assess the risk of harm to affected parties by investigating the circumstances of the Breach. This will include gathering as much information about the Breach as possible.

This assessment will assist in understanding the extent of the risk to affected parties and will help to determine whether the affected parties need to be notified.

Breaches should be assessed on a case-by-case basis as each will be different.

Attachment 1 provides a risk assessment tool.

3. Report the Breach to the relevant authorities

The purpose of reporting is to ensure the right expertise and advice can be applied in any remedial action and intelligence can be gathered and used for future preventions.

Breaches in South Australian government agencies should be reported to the ***Privacy Committee of South Australia***. Attachment 3 provides more information about reporting to the Privacy Committee, including the information required to be reported.

As part of the initial assessment of a Breach, inform all relevant internal parties who may be able to assist with managing the breach. This may include the principal officer, your agency's security team (e.g. Agency Security Executive, Agency Security Advisor, IT Security Advisor) and your agency's privacy team.

If the Breach may be or is a result of an offence, the Breach must be reported **to South Australia Police (SAPOL)** who may provide instructions on how to manage the Breach e.g. whether notifying affected parties should be delayed so as not to compromise an investigation.

The type of information involved, or the way access was attained, may require reporting to additional organisations. For example:

- **SA Government Cyber Security Watch Desk** – for breaches resulting from a cyber security incident. The Watch Desk may be able to help manage the breach (aligning with the SAPSF and SACSF).
- **Office of the Australian Information Commissioner** – for breaches that include tax file numbers.

More information about reporting to additional organisations is in Attachments 3 and 4.

The principal officer of an agency is responsible for notifying affected parties and reporting to the Privacy Committee. In some circumstances, the principal officer may also wish to advise the relevant Minister.

Importantly, reporting should not disclose personal information unless expressly required to resolve the problem. The inclusion of unnecessary personal information would constitute a Breach in its own right. The reporting bodies will usually only need to consider the circumstances around the incident that occurred and the response of the agency.

4. Notify affected parties

The principal officer (usually the Chief Executive) or delegate is responsible for deciding whether to notify affected parties. The default position should always be to notify affected parties as soon as it is practicable to do so, especially if the breach has the potential to cause harm.

However, it may not always be appropriate to notify an affected party of a Breach. In some cases, being made aware of such an incident may cause more harm than the Breach itself.

For example, a Breach notification may cause an individual to disengage from a service. Alternatively, notification of a low-risk Breach may result in unnecessary anxiety or desensitise individuals to further notifications.

Once a decision is made to notify, affected parties should be notified as soon as possible. This provides an opportunity for parties to take immediate action to protect themselves. For example, by changing passwords of accounts and/or being more alert to potential scams resulting from the Breach.

It also demonstrates transparency and is in line with community expectations. People usually expect to be told when their privacy has been breached.

The decision on how to notify should be made on a case-by-case basis. In some cases, agencies may choose to take additional actions that are specific to the nature of the Breach.

When to notify	Those affected should be notified as soon as possible. For Breaches involving an offence or potential offence, check with law enforcement authorities before notifying affected parties or making the details of the incident public so as not to compromise any ongoing investigations.
How to notify	Notify affected parties directly – by phone, letter, email or in person. Indirect notification (e.g. on a website or through a press release) is only appropriate where direct notification is impossible, unfeasible or may cause further harm.
Who should notify	The agency that has a direct relationship with the customer, client or employee should notify those affected. This includes where a Breach may have involved handling of information by a third-party service provider or contractor.
Who should be notified	Generally, the individual(s) or organisation(s) affected by the incident should be notified. In some cases, it may be appropriate to notify an individual's guardian or authorised representative on their behalf.
What should be included in the notification	The information in the notification should help affected parties to reduce or prevent the harm that could be caused by the Breach. This may include: » a description of the Breach » the type of information disclosed » the outcome of the risk assessment » what has been done to respond to the Breach and reduce harm » assistance available to those affected and steps they can take to reduce harm » sources of information that could assist those affected » contact information for the agency where those affected can get more information or address concerns » whether the Breach has been reported to a regulator or other external party » how individuals can lodge a complaint. The wording of the notification may have legal implications and secrecy obligations could also apply. Agencies should consider seeking legal advice. If a separate notification is required under the Australian Data Breaches Notification scheme, e.g. tax file number data has been breached, specific communication requirements apply (www.oaic.gov.au).

When an agency decides not to notify affected parties, they should inform the Privacy Committee of the reason for non-disclosure.

5. Implement remedial action and review

The purpose of taking remedial action is to both limit the impact of the Breach on affected individuals and to prevent further breaches from occurring.

Remedies include the containment, notification and reporting steps already taken, but then review and learn from the Breach to improve personal information handling practices.

This could involve undertaking a review of policies and procedures, increase of or changes to staff training, or even a security review.

Personal Information Breach Response Plan

It is up to each agency how it manages a Breach. A Personal Information Breach Response Plan (plan) can provide guidance and procedures for reporting, recording and investigating information security incidents, which include Breaches. If the agency already has equivalent guidance/documentation, e.g. an incident response plan or policies and procedures relevant to breaches, this may be used in lieu of a plan.

The plan should be developed in accordance with PC030 Protective Security in the Government of South Australia which outlines the whole-of-government approach to protective security by adopting the SAPSF as the protective security policy requirements for the South Australian government. PC030 describes the arrangements and expectations for governance, personnel, physical and information security in South Australian government agencies.

The plan should include:

- what constitutes a Breach – to assist staff in identifying a Breach
- guidance and procedures – to support staff in managing a Breach
- roles and responsibilities of staff – to help staff understand their role and responsibility in managing a Breach
- communications plan – to identify methods of communication to be employed under different circumstances, and
- documentation and review processes – to record Breach events, evaluate how the Breach occurred, how the agency was able to respond and to inform continuous improvement.

All staff should be made aware of the plan.

Attachments

The attachments to this Guideline will assist agencies in assessing the risk of a Breach and the reporting and notification requirements:

1. **Risk assessment** – help in assessing the risk of harm to affected parties and determining the severity of a Breach.
2. **Personal information Breach notification and reporting** – help in determining what information needs to be included in a report, and to whom.
3. **Reporting to the Privacy Committee of South Australia** – requirements of the Privacy Committee for Breach reporting.
4. **Advice organisations** - a list of organisations that you may need to report a Breach or seek further advice about the management of a Breach.
5. **Examples of risk** – a set of case studies addressing different combinations of the risk elements covered in Attachment 1.
6. **Privacy Breach Notification Template**

References

- PC012 Information Privacy Principles Instruction
- PC030 Protective Security in the Government of South Australia
- Office of the Australian Information Commissioner
- Privacy Amendment (Notifiable Data Breaches) Act, 2017 (Commonwealth)

Date approved	Approved by	Version
16/05/2025	Director, State Records	1.0

Need further assistance?

Contact
State Records of South Australia
Tel (+61 8) 7322 7077
Web https://www.archives.sa.gov.au/managing-information/privacy-in-south-australia/personal-information-breaches

Attachment 1: Risk assessment

This table can be used to determine the severity of a Breach and inform the agency, affected parties and appropriate authorities of next steps. (If your agency already has a risk framework in place for use, it is recommended these elements are incorporated).

The outcome of the risk assessment can assist with your notification or report to the Privacy Committee and provides context to the severity of a Breach. The reasons for reporting Breaches to the Privacy Committee include identifying systemic issues, patterns of behaviour within agencies and cultural issues.

Assessment should consider the type of information involved in the Breach, the actual or potential harms that may arise for affected individuals, the seriousness of that harm and the likelihood of that harm occurring.

Each factor taken in isolation may not indicate the overall severity of a Breach. However, when combined, the factors can highlight the risk the Breach may have on affected individuals. For example, a Breach which only affects one individual may not necessarily be low risk. The type of information and who accessed the information may make the Breach a high risk.

This is not an exhaustive list of considerations when assessing the risk of harm, which should be assessed on a case by case basis.

Some hypothetical examples are provided at Attachment 5.

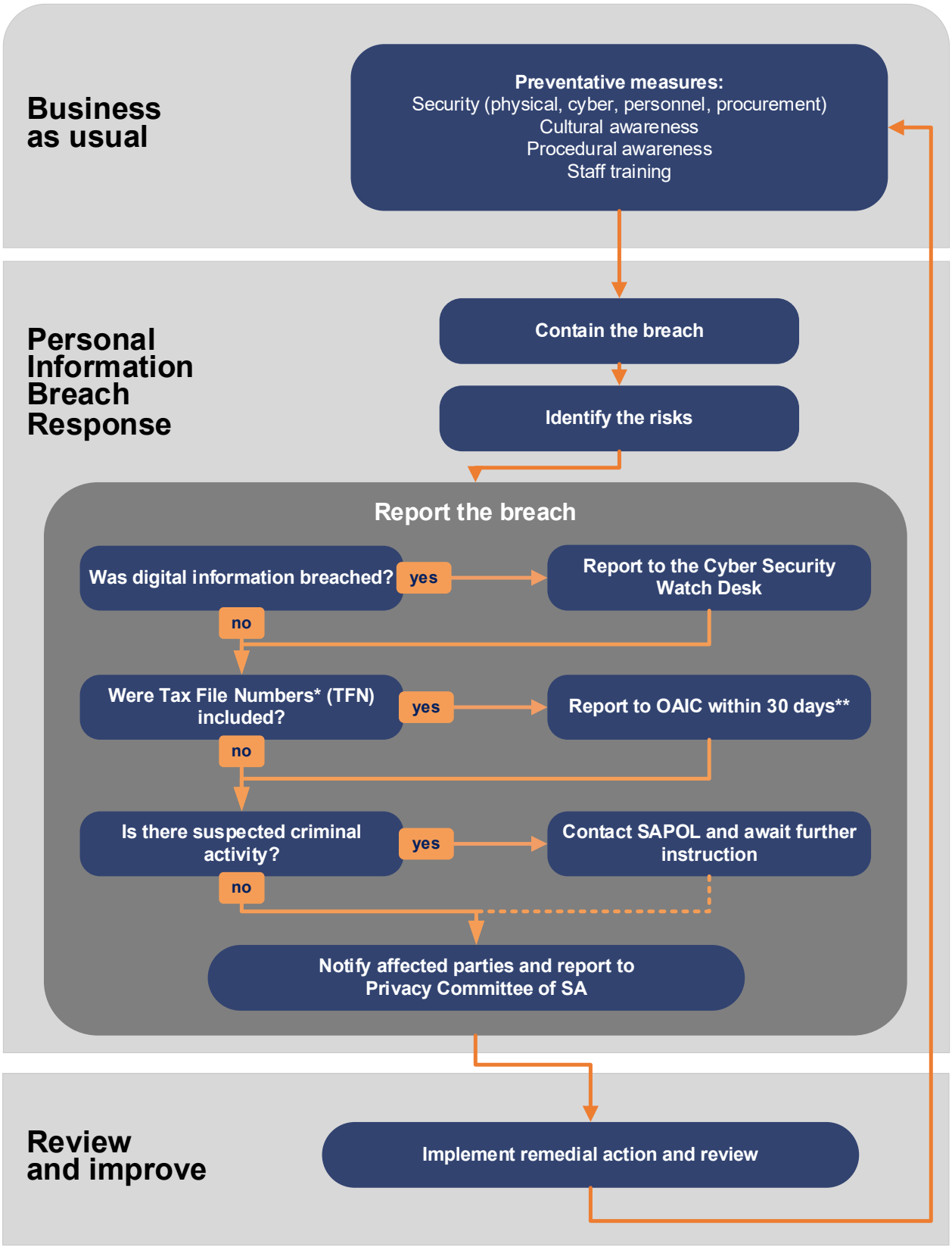
Other factors to consider

Other factors that can impact the severity of a Breach include:

- **Vulnerability of affected parties**
  Agencies should consider whether affected individuals are vulnerable or susceptible to harm. Vulnerability can be temporary or permanent and can arise because of a heightened exposure to harm, or a decreased ability to protect oneself from harm. Vulnerability may be due to a particular attribute or condition of an individual i.e. their age, mental or physical health status, disability status or literacy.
- **Are there any other possible harms that could occur, including to the agency that suffered the incident?**
  It is possible that a Breach could implicate an agency by providing an opportunity to gain access to a secured environment, whether that's physically or digitally.
- **Does this incident highlight compliance issues with other regulations?**
  It is common for a Breach to identify weak points in security protocols, compliance with legislation, records management processes, excessive workloads, or inadequate induction and training.

FACTOR	LOW	MEDIUM	HIGH
Types of information	**Limited** Limited personal information e.g. email address on its own Unopened/returned to sender		**Detailed and/or sensitive** Medical records Financial information Identity documents
What was the security applied to the information?	**High security** Locked secure compactus/cabinets Strong password protections and multi-factor authentication (MFA) or biometrics Strong encryption		**Low security** Accessible to unauthorised individuals Compactus/cabinets unlocked Weak password protection, no MFA or biometrics Weak encryption
How many individuals affected?	**A few** 1-5 individuals		**Many** Hundreds of individuals Quantity unknown
What was the intent of the person who accessed or received the information?	**Accidental** Staff / contractors unintentionally accessing personal information Recipients of emails/letters incorrectly delivered	**Deliberate** Staff / contractors intentionally accessing personal information with benign/limited intent	**Unknown or malicious** Unknown recipients; access uncontained Potential criminal activity Targeted or intentional access
Cause of breach	**Human error**	**Procedural and/or system error**	**Malicious**
How quickly was the breach contained?	**Immediately** Within hours/days		**Unknown, uncontained or a significant length of time**
Potential risk of harm	Nil, annoyance or embarrassment		Identity theft, fraud, physical or emotional harm, harassment, reputational damage, loss of business or employment opportunities, bullying or marginalisation

Attachment 2: Personal information breach notification and reporting



* TFN information is information that connects a TFN with the identity of an individual.

** The *Privacy Amendment (Notifiable Data Breaches) Act, 2017* requires that notifications to individuals affected and the reporting to the Office of the Australian Information Commissioner (OAIC) both contain specific information. See www.oaic.gov.au for more information.

Attachment 3: Reporting to the Privacy Committee of South Australia

Regardless of risk level, all breaches should be reported to the Privacy Committee as soon as practicable, via PrivacyCommittee@sa.gov.au.

The purpose of making a report to the Privacy Committee is so the Committee can:

- keep itself informed as to the extent to which the Information Privacy Principles are being implemented, and
- make recommendations as to the measures that should be taken by the government to improve its protection of individual privacy[3].

The Privacy Committee needs the following information in a Privacy Breach Notification. A template (Attachment 6) is available at Privacy Breach Notification | State Records of South Australia.

A description of the incident	• When did the Breach occur and when did the agency become aware? • What led to the Breach occurring? • Whose personal information and what type of information was involved? [Do not include any unnecessary personal information about affected parties] • Which South Australian government agencies, branches and staff roles were involved? • Were third party organisations or individuals involved?
Advice of the agency response	• What risk of harm exists or existed for affected parties? • Was the principal officer (i.e. Chief Executive) advised of the Breach and when? • Details of communication with affected parties, or the decision not to notify and why. • Details of any support or assistance offered to affected parties. • Implemented or planned changes to training, policies, procedures, systems or culture to prevent a reoccurrence. • Contact details for further correspondence.

The Executive Officer of the Committee can provide general advice on the IPPI and obligations of the reporting agency.

- Phone (Business Hours): (08) 7322 7081
- E-mail (Business Hours): PrivacyCommittee@sa.gov.au

[3] From *Proclamation establishing the Privacy Committee of South Australia*, within the Information Privacy Principles Instruction.

Attachment 4: Advice organisations

These organisations may become involved in responding to a Breach either directly or by offering advice. Reporting a Breach to these organisations may be mandatory.

South Australia Police

If the Breach may have resulted from an offence, a report to SAPOL **must** be made as soon as practicable.

Notification to affected parties may need to be delayed until advice from SAPOL is given, as notification may compromise a criminal investigation.

SAPOL can be contacted on the number below, or visit your local police station:

- Phone (24 hours): 131 444

SA Government Cyber Security Watch Desk, Department of the Premier and Cabinet

All breaches that involve information stored or communicated electronically **must** be reported to the Cyber Security Watch Desk as a cyber security incident.

Information on how to lodge a report can be found at Report a Cyber Security Incident | Security SA.

The Cyber Security Watch Desk can provide advice and assistance on the cyber security aspects of managing a Breach and the consequences of that Breach.

- Phone (24 hours, 7 days a week): 1300 244 168 + 2
- E-mail (Business Hours): WatchDesk@sa.gov.au

State Records of South Australia

State Records and the State Records Council **must** be advised if information assets covered by the *State Records Act 1997* have been lost, damaged or compromised through the Breach incident.

State Records can be contacted on:

- Phone (Business Hours): (08) 7322 7081
- E-mail (Business Hours): staterecords@sa.gov.au
- Website: www.archives.sa.gov.au

State Records also provides executive support to the Privacy Committee.

Office of the Australian Information Commissioner

As per the Australian government's Notifiable Data Breaches scheme (the Scheme) if the Breach relates to TFN information and is likely to result in serious harm, the Office of the Australian Information Commissioner (OAIC) **must** be advised.

The Scheme specifies the information that must be included in the notifications for those affected, the timeframe for notification i.e. as soon as practicable within 30 days of the Breach being discovered and the requirement to report the Breach to the Australian Information Commissioner.

Contact details and information on how to report a Breach to the OAIC can be found at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

IDCARE

IDCARE Official Website | Identity Theft & Cyber Support

If the Breach may result in harm to individuals, they can be referred to IDCARE. The South Australian government has an arrangement with IDCARE to assist with reducing harm to impacted individuals.

Contact DPC at watchdesk@sa.gov.au for more information about this resource.

Additional contacts

You may also need to contact:

- **Any other organisation that is the source of the information that was compromised**. For example, if passport details or Medicare Numbers were contained in the information that was compromised, then the Australian Passport Office or Medicare should also be advised of the Breach.
- **Insurers** such as the SA Government Financing Authority (SAFA) may be required to assess the incident under contractual obligations or to access Cyber Risk Insurance. Claims and incident reporting contact details are posted here: https://www.safa.sa.gov.au/about-safa/contact-us#SAicorp
- **Financial institutions** or credit card companies. This may be to assist you in notifying individuals or reducing the impact on those affected.
- **Regulatory bodies**.
  - Australian Securities and Investment Commission (ASIC). Companies and registered corporations may have reporting requirements to ASIC.
  - Australian Competition and Consumer Commission (ACCC). The ACCC has a role in protecting the interests and safety of consumers and as such they have their own Breach notification requirements.
  - Australian Communications and Media Authority (ACMA). ACMA have their own breach reporting requirements if the compromised information includes Integrated Public Number Database information.
- **Other internal or external parties**. Consider if any other third parties may have been affected by the Breach. For example, if information about a particular government tender process was breached, all organisations that submitted a tender, even if their information wasn't included in the Breach, may need to be notified. Some parties to consider include:
  - other internal business units not already notified that may have a need to know (e.g. communications, human resources, senior management group, risk committees)
  - other government departments that may experience some impact from the Breach, or
  - unions or other employee representatives, particularly if any employee information was compromised.
- **Office for Public Integrity and the South Australian Ombudsman.** These organisations deal with corruption, misconduct and maladministration.

Other regulatory bodies

Your agency may need to report or notify other regulatory bodies specific to your sector. For example, if water licensing information is compromised, the agency may be required to notify water licensing regulatory bodies or boards. The education, infrastructure, health, justice and child protection sectors, in particular, may have specific regulatory bodies that require advice in the case of a Breach.

Attachment 5: Examples of risk assessments

The following examples are based on plausible, hypothetical scenarios. They highlight the combinations of risk elements covered in Attachment 1.

High risk incident #1

A third party contracted service provider informed several of their South Australian government client agencies of a security breach in which data was stolen from their systems.

The information was dated between 2012 and 2022, covered over 30,000 clients and included identified and de-identified data tables involving name, home address, financial information (service charges and concessions, not banking details), service codes and service outcome information.

They were informed that data from 'other South Australian government, Commonwealth government and private sector clients' was included in the theft, including another department managing a similar client data set.

The Office of the Australian Information Commissioner (OAIC) had been informed and was forming a response team along with police and cyber security contacts.

Types of information	Name, contact details, service charges and concessions, indications of medical conditions, service outcomes (qualitative). Able to be merged with another stolen data set.	**HIGH**
What was the security applied to the information?	Stored on a secure server but accessed through a weak security point. Stored under quarantine from other data sets but multiple data sets have been stolen by the same operator. Data tables partially codified, but with the code key, not encrypted.	**HIGH**
How many individuals affected?	30,000 in one agency, several thousand in other agencies	**HIGH**
What was the intent of the person who accessed or received the information?	Criminal agent, malicious intent	**HIGH**
Cause of the breach	Malicious	**HIGH**
How quickly was the breach contained?	Unclear, however the most recent stolen data is from 2022, indicating the breach occurred some time ago and is uncontained.	**HIGH**
Potential risk of harm	Identity theft, fraud, physical or emotional harm, harassment, reputational damage, loss of business or employment opportunities, bullying or marginalisation	**HIGH**

Given the interaction between each of the factors, the overall risk was assessed as HIGH.

Response

The contracting party worked closely with the OAIC in identifying the risks to the impacted data and with police and cyber security experts to identify the intruder and scope of the theft.

Investigations into the operations of the third-party contractor found no breach in contractual agreements or security protocols but recommendations from a post-incident review were shared with the other client agencies and Procurement Services.

Regular advice was provided to the Ministers responsible for each of the SA government agencies, as well as the Treasurer and the Attorney-General. Post-incident review information will be taken on board to improve future prevention.

Each agency was encouraged to undertake a review of other high-risk data stored with contractors and consider implementing instructions to return and delete residual holdings and manage their own data holdings in accordance with a disposal schedule under the *State Records Act 1997*.

Notifying affected parties

The OAIC coordinated a standardised approach for notifying affected parties. The agency with the closest association with each party would be responsible for contacting those clients.

The affected client details were checked against other information sets to identify any who had passed away, had changed address or state, or were now under the care of a guardian or power of attorney.

Message content was developed in consultation with the OAIC, DPC Cyber Security, the Privacy Committee and strategic communications and media teams for each of the affected agencies.

DPC Cyber Watch Desk engaged IDCare to support the notification and harm reduction process.

High risk incident #2

While delivering several cardboard boxes of records to an off-site storage provider, the courier van was involved in an accident, resulting in one of the boxes, which was old and torn, spilling onto the road. Pages were seen blowing across a major roadway and could not be safely recovered. Once the rest of the records were recovered, it was identified the missing papers were from a folder of handwritten medical reports for at least 30 consumers, assessed 5 years prior. Many of the recovered medical records included detailed information about patients' mental and physical health conditions.

Types of information	Medical records (detailed)	**HIGH**
What was the security applied to the information?	Boxes were damaged and documents were not sufficiently secured during transportation	**HIGH**
How many individuals affected?	At least 30	**MEDIUM**
What was the intent of the person who accessed or received the information?	Unknown – documents not recovered.	**HIGH**
Cause of breach	Human error	**LOW**
How quickly was the breach contained?	Uncontained.	**HIGH**
Potential risk of harm	Unclear, however the individuals affected by the breach may be vulnerable, given the recovered records contain detailed medical information. This could make them susceptible to emotional harm, loss of business or employment opportunities, bullying or marginalisation.	**HIGH**

Given the interaction between each of the factors, the overall risk was assessed as HIGH.

Notifying affected parties

There was no way of finding out which consumers' reports had been lost, as they were the only copy of the records, and it was too difficult to compare the recovered records with admission registers from the time. Making a public statement would cause significant concern amongst people who were not necessarily affected. The consumer complaints team was advised in case any complaints were raised.

Response

The loss of official records was reported to State Records. This incident highlighted a problem with past records management practices which did not involve registering medical reports, and weak storage security.

While the registration processes have since improved, a new documentation step has been added to the process for transferring older records to off-site storage. To prevent future incidents, documents were stored in more secure containers.

Medium risk incident #1

On discharge from hospital, a patient was handed a copy of their discharge paperwork. When they got home their carer realised the paperwork had the name, address and date of birth of another person. As both patients had a similar procedure, the discharge notes seemed to broadly match this patient, with some variations regarding medication.

They called the hospital and were asked to return the papers to the hospital in-person or through the post and were advised the correct discharge papers would be posted to them. The patient offered to shred the papers, but the hospital explained they would need to investigate the cause of the mix up.

Types of information	Medical records (contact information, treatment plans and medications)	**HIGH**
What was the security applied to the information?	Unlikely that thorough identity checks were conducted.	**HIGH**
How many individuals affected?	1 or 2	**LOW**
What was the intent of the person who accessed or received the information?	Accidental – an unauthorised recipient who was also a client of the same service	**LOW**
Cause of breach	Human error	**LOW**
How quickly was the breach contained?	Within days	**LOW**
Potential risk of harm	Annoyance, possible emotional harm depending on the kind of medical details included. Misapplication of another person's medical advice could lead to physical harm.	**MEDIUM**

Given the interaction between each of the factors, the overall risk was assessed as MEDIUM.

Notifying affected parties

Once the paperwork was returned and the details of the other patient were confirmed, a phone call was made to the other patient to explain the disclosure. They had been given their own records on their own discharge. They were offered an apology and contact details for making a complaint if they wished. They accepted the apology and said they were not overly concerned about the mistake.

Response

It was discovered the discharge papers for the other patient had been printed twice and so was assumed the second set belonged to the reporting patient.

Staff on the ward were reminded of the importance of a three-point identity check before handing over papers.

Low risk incident #1

An email intended for a manager in the team was accidentally sent to someone with the same surname from another SA public sector agency. The email included information from a staff member seeking to book leave over the end of year period, with a query about long-term planning.

The recipient notified the sender of the error and confirmed they had deleted the email, and they had not onforwarded it.

Types of information	Informal leave request	**LOW**
What was the security applied to the information?	Email, unencrypted, no password protection.	**HIGH**
How many individuals affected?	1	**LOW**
What was the intent of the person who accessed or received the information?	Unauthorised staff member within the SA Public Sector	**LOW**
Cause of breach	Human error	**LOW**
How quickly was the breach contained?	Within hours	**LOW**
Potential risk of harm	Nil or annoyance	**LOW**

Given the interaction between each of the factors, the overall risk was assessed as LOW.

Notifying affected parties

At the Manager's discretion, it was decided to notify the affected staff member, and this was done during a 1:1 meeting, with an explanation and apology.

Personal Information Breach Notification

Email completed notification to the Privacy Committee of South Australia (PCSA) via privacycommittee@sa.gov.au ASAP after agency becomes aware of breach.

Do not include any unnecessary personal information within this notification.

Contact Details

Name			
Title			
Email		**Phone number**	

Agency Details

Agency name	
Business unit	
Name and title of principal officer (e.g. CE) or delegate	
Additional agencies or organisations involved (if applicable). **Have they notified the PCSA separately?**	

Incident details

When did the breach occur?		
What date did the agency become aware of the breach?		
Agency reference for the incident (e.g. SAHI or document ref)		
How did the agency become aware of the breach? (e.g. complaint, staff observed, system fault)		
What date was the principal officer advised?		
How did the incident breach the Information Privacy Principles? **(select all that apply to the incident)**	☐ Collection ☐ Disclosure	☐ Storage ☐ Use

Incident description

Please provide a description of the incident.

Other reports

Has a report been made to the DPC Cyber Watch Desk?	☐ Yes	☐ No	☐ NA
Has SAPOL been advised?	☐ Yes	☐ No	☐ NA
Did the incident involve Tax File Numbers?	☐ Yes	☐ No	☐ NA
(If yes, has a report been sent to the OAIC?)	☐ Yes	☐ No	

Incident risk factors

Please refer to the Personal Information Breach Guideline Attachment 1 when assessing these risks.

Date assessment commenced			
Types of information included (Include elements like "DOB" or "passwords")	☐ High	☐ Medium	☐ Low
Description:			
Security applied to the information	☐ High	☐ Medium	☐ Low
Description:			
Number of individuals affected	☐ High	☐ Medium	☐ Low
Number:			

Who accessed or received the information and what was their intent?	☐ High	☐ Medium	☐ Low
Description:			
Cause of breach	☐ High	☐ Medium	☐ Low
Description:			
How quickly was the breach contained	☐ High	☐ Medium	☐ Low
Description:			
The potential risk of harm	☐ High	☐ Medium	☐ Low
Description:			
Were the affected parties vulnerable or susceptible to harm? If so, how?			
Are there other possible harms that might occur to the agency?			
Has this breach highlighted compliance issues with other regulations?	☐ Yes	☐ No	
OVERALL RISK ASSESSMENT	☐ **High**	☐ **Medium**	☐ **Low**

Notifying affected parties

Have the affected parties been notified?	☐ Yes	☐ No
If not, why not?		
What actions have been taken to limit the impact on affected parties?		
What actions have been taken to offer support or assistance to the affected parties?		

Remediation

Actions have been taken to remediate the impact on affected parties and offer support and assistance.	☐ Yes ☐ No
Response plan actions:	
What actions have been taken to prevent future breaches?	

Additional comments