Protecting sensitive personal information

You are responsible for handling all work information with integrity and, in particular, protecting sensitive personal information.

Legal requirements to protect

Public sector organisations collect and store a large amount of information about staff, clients, patients and customers.

The purpose of the *Personal Information Protection Act 2004* (Tas)[1] (the Act) is to protect the privacy of individuals by controlling the ways in which the government can collect, keep, use, and release records containing sensitive personal information that clearly identifies an individual. The Act also enables individuals to access that information.

Personal Information Protection Principles

An important part of the Act is the personal information protection principles. All Tasmanians, including public sector employees who are custodians of personal information, must comply with these principles. They cover:

- collection
- use and disclosure
- data quality
- data security
- openness
- access and correction
- unique identifiers
- anonymity
- disclosure of information outside Tasmania, and
- sensitive information.

Your organisation's responsibilities

As a public sector employee, you work within an employment framework that includes various legal requirements (such as the Code of Conduct or a similar code).

To protect you and the individuals whose personal information it collects, your organisation should have policies, procedures, protocols, and guidelines.

You must follow them at all times.

What is sensitive personal information?

The Act defines personal information as:

- any information or opinion in any recorded format about an individual –
  - whose identity is apparent or is reasonably ascertainable from the information or opinion, and
  - who is alive or has not been dead for more than 25 years.

Basic personal information is a person's name, residential address, postal address, date of birth and gender.

Sensitive personal information

The term 'sensitive information' is often used interchangeably with 'confidential information', which covers a much broader range of information types, including personal, commercial and legal.

For this fact sheet, sensitive information refers to sensitive personal information. See our other fact sheet on 'Managing confidential and protected information'.

According to the Act, sensitive information is:

- personal information or an opinion relating to personal information about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association
  - membership of a trade union
  - sexual preferences or practices, and
  - criminal record
- health information about an individual.

Managing sensitive personal information

The collection of sensitive information about an individual requires the individual's consent. There are circumstances when an employee may collect sensitive information without consent, such as to save the individual's life.

Protecting sensitive information

Various legislation requires public sector organisations to take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. They also must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.

Disclosing sensitive information

In general, public sector employees may only use or disclose personal information about an individual for the purpose for which it was collected. Your organisation's policies and procedures should provide more detail about any exemptions to this rule.

Misusing sensitive personal information

Members of the public should be able to trust that public sector organisations will deal with their sensitive information appropriately and according to legislative and policy requirements. Failure to do so may damage the reputation of the organisation and government and could lead to legal action.

Unintentional misuse

Misuse of sensitive information can occur due to unintentional errors or oversights by employees, for example, when a storage device is misplaced or an employee incorrectly addresses an email to the wrong recipient.

You mustn't hide or ignore any errors when handling sensitive information. Follow your organisation's procedures about such incidents and immediately inform your manager.

CASE STUDY

On 25 November 2013, the Office of the Australian Information Commissioner (OAIC) was notified that boxes of unsecured medical records had been found in a garden shed at an address in Narre Warren South (Victoria). Thieves had broken into the shed and as a result the boxes of medical records were compromised (data breach).

The owner of the site – a medical centre – estimated there were paper-based health records for approximately 960 patients stored in the shed, and therefore that at least 960 individuals' personal information was compromised in the data breach.

The medical centre advised the OAIC that patient health records were transferred from the locked room inside the former premises to a garden shed at the back of the site (so that renovations for sale of the site could occur). The garden shed door had been locked with padlocks.

The Commissioner found that the medical centre did not take reasonable steps to protect the personal information, some of which was also sensitive information.

Extracted from Office of the Australian Information Commissioner report[2]

Loss of information

A loss of information or data occurs whenever information or data is unaccounted for or cannot be located. An example is when a staff member leaves the organisation without transferring data access.

Failure to de-identify

Failure to de-identify occurs when a piece of information has not had all identifying information about a person removed. Such negligence can occur in two ways:

- by failing to remove a person's name from the relevant information, or
- by removing the person's name but failing to remove other identifying information, such as their address, age or physical features, that would allow another person to make an educated guess as to their identity.

Failure to destroy

A serious form of misuse is when information intended to be removed from access by destruction is not actually destroyed.

While losing data or failing to destroy may seem harmless, both can lead to the same outcome as someone deliberately releasing sensitive information. They are therefore treated just as seriously.

Intentional misuse

Public sector employees who improperly access sensitive information from public sector databases can be motivated by many things. Sometimes, curiosity is the sole motivation, but even this may be considered misconduct.

In serious instances, perpetrators may access data with the intention of passing it on to others, profiting from it, or frustrating investigations or proper legal processes.

Impact on victims of misuse

Misuse of sensitive information can cause harm to individuals. It can be physical, financial, emotional or reputational. Examples of possible harm are:

- reputational damage, embarrassment or humiliation
- emotional distress
- identity theft or fraud
- financial loss
- loss of employment or business opportunities, and
- family violence or other physical harm and intimidation.

CASE STUDY

A former Queensland Health employee (the complainant) had her patient file accessed multiple times by a colleague (the respondent) without there being a work-related purpose for doing so. It became apparent the respondent knew about the complainant's sensitive health information.

Following an audit of access to the complainant's patient file (carried out at the request of the complainant), it was revealed that other members of staff had also accessed the complainant's file.

The complainant suffered from nightmares, high levels of anxiety, was fearful of staff continuing to browse her health information, and ultimately lost complete trust in the agency.

Extracted from Queensland CCC report, 'Operation Impala'[3]

Follow your workplace policies, procedures and guidelines

You must always comply with the policies and procedures and any other guidance and training you receive concerning work information. If you feel uncertain about any matter, seek advice from your manager.

---

[1] www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046#JS1@EN

[2] www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information

[3] www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf

The Commission can help

We are available to provide support and assistance with identifying, reporting, investigating, managing and preventing misconduct: prevention@integrity.tas.gov.au or 1300 720 289.

For more Misconduct Prevention resources go to www.integrity.tas.gov.au/resources