

Department of Health Privacy Policy

Meeting legislative privacy obligations

OFFICIAL

Contents

Overview	2
To what and whom does this policy apply?	2
What does the department do?	3
Definitions of personal, health and sensitive information	3
Personal information	3
Sensitive information.....	3
Health information	4
Collection of personal and health information	5
Collection of sensitive information	6
Types of information collected by the department	6
What the department does with the information collected.....	6
Linking of data	8
How the department stores and protects information	8
Access to and correction of information	8
Making a complaint about a privacy incident (breach)	9
Protecting information transferred outside of Victoria	9
Workplace participant responsibilities	10
Relevant legislation	10

OFFICIAL

Overview

The Department of Health (department), along with its funded and contracted service providers, collects, uses and discloses personal information (which includes sensitive information) and health information about its staff and people using its services.

The department acknowledges the sensitivity of personal and health information provided to it. Therefore, the department is committed to protecting the privacy of this personal and health information in accordance with the law.

The department is bound by privacy and other laws, including:

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Freedom of Information Act 1982*
- *Victorian Data Sharing Act 2017*
- *Public Records Act 1973.*

Using and disclosing information about clients is a legitimate part of providing services and keeping people safe.

However, it is important to note that information may only be dealt with in accordance with the law.

Information on website privacy can be found on the [Website privacy statement](#) page, and more information can also be accessed on our [Privacy](#) page.

To what and whom does this policy apply?

This policy applies to all personal and health information collected, stored, used and disclosed about any individual including:

- clients
- patients of health service providers
- people registering for services.

This policy also applies to all personal and health information collected, stored, used and disclosed about people working for the department, including:

- department staff
- secondees
- labour hire
- personnel
- contractors and sub-contractors
- those on work experience and volunteers.

These individuals are collectively referred to throughout this document as workplace participants.

What does the department do?

The department supports and enhances the health and wellbeing of all Victorians, leading and shaping the health sector through policy, service design and delivery.

The services and functions that we and our funded and contracted service providers deliver include:

- hospitals and health services
- primary and community health
- public health
- mental health
- alcohol and drugs
- ageing and aged care.

The department collects, uses, stores and discloses a range of personal and health information for the purposes of providing services or to carry out its statutory functions.

Definitions of personal, health and sensitive information

Personal information

Personal information is defined in the Privacy and Data Protection Act as:

- information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act applies.

Sensitive information

Sensitive information is a subset of personal information. It is defined in the Privacy and Data Protection Act.

It means information or an opinion 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, orientation or practices
- criminal record

that is also personal information.

Health information

Health information is defined in the Health Records Act.

Where information is health information and so is not caught by the Privacy and Data Protection Act, the privacy law that regulates it differs in some respects.

The Health Records Act defines health information as:*

- information or an opinion about:
 - the physical, mental or psychological health (at any time) of an individual; or
 - a disability (at any time) of an individual; or
 - an individual's expressed wishes about the future provision of health services to him or her; or
 - a health service provided, or to be provided, to an individual

that is also personal information (see definition of personal information under the *Health Records Act 2001* below);

or

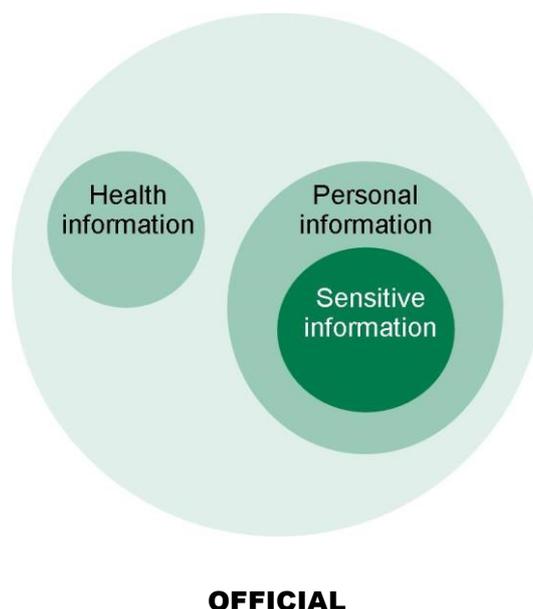
- other personal information collected to provide, or in providing, a health service; or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants.

*The definition does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the Health Records Act generally or for the purposes of specified provisions of that Act.

Personal information is defined in the Health Records Act as:

- 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, but does not include information about an individual who has been dead for more than 30 years.

Figure 1. Relationship between personal, sensitive and health information



Collection of personal and health information

The department collects personal and health information necessary to the department's functions and activities, including various programs and services it runs and those it funds others to provide and/or that the department regulates.

The department collects personal and health information only by lawful and fair means and not in an unreasonably intrusive way.

If it is reasonable and practicable to do so, the department collects personal and health information about an individual only from that individual.

When collecting information directly from an individual and when collecting information from someone else about an individual, the department will take reasonable steps to ensure the individual is aware of:

- why the information is being collected (including the purposes for the collection and any relevant laws requiring the collection)
- who it may be disclosed to, the main consequences if the individual does not disclose the information (if collecting information directly from the individual)
- how the individual may contact the department and gain access to the information collected.

There may be exceptions in the Information Privacy Principles and the Health Privacy Principles in certain circumstances that do not require reasonable steps to be taken but this needs to be assessed on a case by case basis.

The department typically collects information in the following ways:

- directly from the individual to which the information relates
- where it is not reasonable or practicable to collect the information directly from the individual, information may be collected from a third party, such as the individual's authorised representative
- as a by-product of service delivery, which may include through funded agencies (such as health services) which are required to provide the information to the department for the purpose of the department's functions and activities (usually included in extracts from their electronic systems)
- as a result of activities associated with
 - registrations
 - board appointments
 - processing applications for services
 - sporting activities and grants
 - mandatory reporting (such as for notifiable diseases, cancer registration)
- where information may be provided by a third party.

The department collects personal and health information for delivering, planning, funding, monitoring, evaluating and improving our services and functions, and for meeting statutory requirements.

Unless the use or disclosure of personal or health information is for the primary purpose of collection, or it is for a secondary purpose and one of the permissible exceptions under Information Privacy Principle 2.1 or Health Privacy Principle 2.2 applies, the department ordinarily removes identifying details from the information it collects.

Collection of sensitive information

The department may collect sensitive information where:

- the individual has consented to the collection,
- the collection is required or authorised under law,
- the collection is necessary to prevent or lessen a serious threat to the life or health of any individual,
- where the individual whom the information concerns is physically or legally incapable of giving consent to the collection or physically cannot communicate consent to the collection, or
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

The department may also collect sensitive information about an individual if:

- the collection is necessary for research or the compilation or analysis of statistics relevant to government funded targeted welfare or educational services, or
- the information being collected relates to an individual's racial or ethnic origin and the purpose of the collection is to provide government funded targeted welfare or educational services, and

there is no reasonably practicable alternative to collecting the information for either purpose, and it is impracticable for the department to seek the individual's consent to the collection.

Types of information collected by the department

The types of personal or health information the department collects depends on the nature of the contact with the department, services provided (where applicable) and statutory requirements of the department.

Personal information collected by the department may include (but is not limited to):

- name, address and contact details
- personal circumstances (age, gender)
- financial matters (payment and bank account details)
- identity (date and country of birth)
- government identifiers.

The department also collects health information where necessary to carry out its functions or activities, for example:

- regulatory functions such as approval of permits
- funding, management, planning, monitoring, improvement or evaluation of health services.

What the department does with the information collected

The department uses and discloses personal (including sensitive) and health information for:

- the primary purpose for which it was collected; or
- a secondary purpose where the legislative requirements for using or disclosing for a secondary purpose are met.

The department may use or disclose personal (including sensitive) or health information when:

- the secondary purpose relates to the primary purpose of collection (or directly relates to the primary purpose in the case of sensitive or health information) and an individual would reasonably expect the department to use or disclose it in this way,
- the individual to whom the information is about has given consent for the use or disclosure, or
- the department is required, authorised or permitted by or under law to use or disclose the information.

The information collected may be shared within the department between different business units if business units comply with the Information Privacy Principles and the Health Privacy Principles.

Such information may also be shared by the department to service providers to enable efficient and effective delivery of quality services, or for the funding, management, planning, monitoring, improvement or evaluation of health services, in compliance with the Information Privacy Principles and Health Privacy Principles.

The department may also share with other government departments or agencies in accordance with applicable privacy laws.

The department collects, uses, holds and discloses personal and health information about a range of matters, including, but not limited to:

- individuals participating in funded services
- managing contracts and funding agreements
- managing fraud and compliance investigations
- managing audits
- managing grants
- employment and personnel matters concerning department staff and contractors
- correspondence from members of the public to the department, Ministers and Parliamentary Secretaries
- complaints made and the feedback provided
- requests made under the Freedom of Information Act 1982
- investigating incidents, for example health protection matters
- planning, monitoring and evaluating departmental functions and services
- meeting legislative requirements
- policy development and research
- meeting the reporting requirements of government and external oversight agencies
- mandatory reporting of certain diseases.

There are circumstances where the department is authorised and/or required by law to collect, use, hold or disclose an individual's information.

Wherever it is lawful and practicable, an individual must be given the option of remaining anonymous when interacting with the department. A circumstance where it is not practicable for the individual to remain anonymous is where the department is responsible for providing a full range of specific and coordinated services to the individual.

The department will not assign unique identifiers to individuals unless the assignment is necessary to enable it to carry out its functions efficiently or is otherwise required by law. It will only adopt (as its own unique identifier of an individual), use or disclose a unique identifier assigned by another organisation in limited circumstances.

OFFICIAL

Linking of data

In order to better inform department services and policies, the department may link data that it has collected. Where this occurs, the department combines multiple pre-existing datasets into a single linked dataset, which can then be used for policy development, statistical research and evaluating current and future services.

Statistical data and trends identified from this may be provided to other government bodies and agencies to promote the health and wellbeing of Victorians.

Any personal or health information used in the data sets will have been lawfully collected by the department or other agencies, and the subsequent use of that data to create a linked dataset, and disclosure of that linked dataset, will only occur where this is in compliance with law.

Often data linkage will involve de-identifying data beforehand to ensure that it is not traceable to an individual, and this de-identification will only be done where it is in compliance with law.

Example of data linkage

An example of a data linkage project is where the department, in conjunction with the VCS Foundation, is collating breast, bowel and cervical cancer screening data. These data are regularly collected under state and commonwealth legislation, and with individuals' consent.

Integrating multiple sources of key cancer screening data sets will provide comprehensive reporting, monitoring and interpretation of cancer screening programs in Victoria.

When linked by the VCS Foundation (on behalf of the department), in de-identified form, the data will show population and program trends to enable reporting against the screening and early detection priority areas of the Victorian Cancer Plan, for the purpose of better service planning and program delivery.

How the department stores and protects information

The department has security measures designed to protect personal and health information from misuse, loss, unauthorised access, modification or disclosure.

The department must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose in line with the Public Records Act 1973.

In relation to health information, the department must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by the Health Records Act, the regulations made under the Health Records Act, or any other law.

The department takes reasonable steps to ensure that any personal and health information it collects, uses and discloses is accurate, complete and up to date, and having regard to the purpose for which health information is to be used, that it is relevant to the department's current functions and activities.

Access to and correction of information

An individual may ask for access to their information or request a correction to their information by contacting the department through:

- their case manager (where applicable)
- the department area that has the information (where known)
- contacting the Freedom of Information Unit by email at foi@health.vic.gov.au or by phone on 1300 020 360

When contacted, the department will let the individual know whether it holds information about the individual and any further steps that that individual should take to obtain access to the information.

If a query relates to an individual's health information, this information will be held directly by the public health service provider. In this situation it would be more appropriate to make contact directly with the health service provider.

Making a complaint about a privacy incident (breach)

An individual may make a complaint about a potential privacy incident (breach) by emailing the department's Privacy and Legal Compliance team in Legal Services at privacy@health.vic.gov.au.

The team can also provide advice in relation to information sharing and privacy matters for department staff.

The department undertakes to resolve privacy complaints and breaches in a timely and fair manner.

An individual may also make a privacy complaint to:

- the Health Complaints Commissioner (HCC) in relation to a complaint relating to health information:
 - address: Level 26, 570 Bourke Street, Melbourne VIC 3000
 - phone: 1300 582 113
 - website: www.hcc.vic.gov.au
- the Office of the Victorian Information Commissioner (OVIC) in relation to a complaint relating to personal or sensitive information:
 - address: PO Box 24274, Melbourne VIC 3001
 - phone: 1300 006 842
 - email: enquiries@ovic.vic.gov.au
 - website: www.ovic.vic.gov.au

HCC resolves complaints about healthcare and the handling of health information in Victoria. It can also investigate matters and review complaints data.

OVIC provides independent oversight of the Victorian public sector's collection, use and disclosure of public sector information. Its functions include resolving privacy complaints through a conciliation process.

Protecting information transferred outside of Victoria

The department adheres to the requirements of the *Privacy and Data Protection Act* and the *Health Records Act* when transferring personal and health information outside of Victoria.

The only circumstances in which personal and health information may be transferred or stored outside of Victoria is when the transfer or storage meets one (or more) of the following criteria:

- the department reasonably believes that the recipient of the information is subject to a law, binding scheme or binding contract that provides substantially similar protection to the Privacy and Data Protection Act or Health Records Act
- the individual has provided consent to the transfer
- the transfer is necessary for the performance of a contract between the individual and the department, or for the implementation of pre-contractual measures taken in response to the individual's request

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the department and a third party
- the transfer is for the benefit of the individual, and it is impracticable to obtain the individual's consent to the transfer, but if it were practicable to obtain consent the individual would be likely to give it
- the department has taken reasonable steps to ensure that information which it has transferred will not be held, used or disclosed by recipients inconsistently with the Information Privacy Principles or Health Privacy Principles
- in the case of health information, the transfer is required or authorised by law.

Workplace participant responsibilities

It is every workplace participant's responsibility to familiarise themselves with the Information Privacy Principles set out in the Privacy and Data Protection Act and the Health Privacy Principles set out in the Health Records Act and to ensure that they comply with them.

Relevant legislation

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Freedom of Information Act 1982*
- *Victorian Data Sharing Act 2017*
- *Public Records Act 1973*

These Acts are available on the Victorian Legislation and Parliamentary Documents website via www.legislation.vic.gov.au by searching under 'Victorian Law today.'

To receive this publication in an accessible format email the Privacy and Legal Compliance team at privacy@health.vic.gov.au.

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.

© State of Victoria, Australia, Department of Health, October 2022. This version replaces the June 2021 version. Available at [Privacy \(health.vic.gov.au\)](http://Privacy.health.vic.gov.au)

Version History from 10 October 2022. Reviews prior to this date not captured.

Version	Date	Summary of changes
2022.1	25 October 2022	Minor edits to improve clarity and update contact information.