ESTA 000

POLICY

Privacy Policy

#Iam000

Document information

Name of policy		Privacy Policy	
Description of policy		To outline ESTA's policy for the management of privacy	
Policy applies to		☒ ESTA wide ☐ Specific (*outline location, site, organisational unit etc.)*	
		☒ All Employees	☐ Nominated Employees
Policy status		☐ New	☒ Revision
Description of revision	14/7/15	V1 Initial Draft	
	27/8/15	V1.1 updated feedback from KPMG	
	28/9/15	V1.2 Legal review	
	18/12/15	V1.3.Document amended and redrafted	
	24/8/16	V1.4 Final Approved by ELT	
	14/12/18	V 1.5 updated format	
	3/9/20	V 1.6 Document reviewed by General Counsel and Board Secretary	

Document author	General Counsel and Board Secretary
Document owner	General Counsel and Board Secretary
Document type	Policy
Creation date	July 2015
Revision Date	3 September 2020

Approved by	Board
Approval date	19 November 2020
Effective date	6 June 2019
Date of next revision	June 2022
Frequency of review*	2 years

** Unless otherwise indicated, this policy will still apply beyond the review date.*

Related documents: legislation, policies, procedures, guidelines and local protocols	• *Privacy and Data Protection Act 2014 (Vic)* • *Emergency Services Telecommunication's Act 2004 (Vic)* • *Health Records Act 2001 (Vic)* • *Freedom of Information Act 1982 (Vic)* • *Victoria's Charter of Human Rights and Responsibilities Act 2006 (Vic)* • ESTA's Code of ethics • Code of Conduct for Victorian Public Sector employees • Information Security Policy • Managing Misconduct policy • SECC control room access • Media Management Policy • Risk policy • Enterprise Risk Management framework

Table of Contents

1 ESTA's commitment to information privacy

ESTA is committed to protecting the privacy of personal information that we handle in the delivery of services to the community, agencies, employees and agents. The way ESTA collects discloses and manages personal and health information contributes to its success.

Victoria has three key pieces of legislation: the *Emergency Services Telecommunications Act 2004*; the *Privacy & Data Protection Act 2014*; and the *Health Records Act 2001* which apply to ESTA. These laws contain information about confidential information, and privacy principles which give people more say in regard to how their personal and health information is collected and used and who can access it.

In addition, Victoria's Charter of Human Rights and Responsibilities protects individuals from having their privacy unlawfully or arbitrarily interfered with.

2 Policy Statement

Protecting and enhancing information privacy supports ESTA in delivery of its objectives and aligns with organisational and public sector values. The application of a consistent information privacy compliance regime at ESTA will provide assurance that policies and procedures:

- Comply with relevant legislative and regulatory requirements
- Encourage a high level of awareness and accountability at all levels of the organisation
- Support ESTA strategic and business objectives.

2.1 Policy objectives

This policy and related procedures will assist ESTA:

- Improve awareness of the privacy principles relating to personal and health information in the ESTA context
- Provide guidance regarding individual and organisational compliance with privacy legislation and privacy principles
- Build greater transparency, improved communication and training, tracking and reporting of privacy activities.

2.2 Purpose

The purpose of this policy is to articulate ESTA's information privacy philosophy and the processes and practices in place to assist ESTA in achieving its goals and objectives. The Policy also ensures that responsibilities are appropriately delegated for privacy management.

3 Governance

ESTA's governance structure relating to information privacy is set out below. This structure illustrates ownership of the policy and roles and responsibilities for the information privacy at ESTA.

3.1 Ownership

The Privacy Policy is endorsed by the Executive Leadership Team (ELT) and owned by the Board Secretary who performs the duties of Privacy Officer at ESTA and is responsible for its privacy framework

3.2 Privacy framework and strategy

ESTA's Privacy Policy fits within the wider Privacy Framework, supported by an active strategy to improve privacy compliance and awareness at ESTA.

LEGISLATION

- **Emergency Services Telecommunications Authority Act 2004**
- **Privacy and Data Protection Act 2014**
- **Health Records Act 2001**
- **Freedom of Information Act 1982**

REGULATORS

- **Minister for Emergency Services**
- **Information Commissioner**
- **Privacy & Data Protection Deputy Commissioner**
- **Public Access Deputy Commissioner**
- **Health Complaints Commissioner**

Compliance	Information, Advice & Guidance	Training & Awareness	Monitoring, Reporting, Managing
Compliance with privacy laws and privacy principles, and other relevant legislation and policy	**Provision of advice and guidance internally and externally regarding privacy rights and responsibilities**	**Training and awareness activities within the organisation**	**Monitoring, reporting and managing privacy practice including incident management**
Includes: • Legislation • Information Privacy Principles • Health Privacy Principles • Privacy Policy and related policies • Data Security & Management	Includes: • Provision of policy & related information on internal & external websites • Information & guidance regarding making complaints & managing breaches	Includes: • Organisation-wide privacy training online • Regular bulletins and information updates regarding Privacy at ESTA • Targeted information for managers.	Includes: • Monitoring • Reporting • Review processes • Complaint and breach management • Incident management
Roles & Responsibilities • All ESTA Employees • All contractors, suppliers and others involved in delivery of ESTA's operations who have access to personal or health information	Roles & Responsibilities • Board Secretary • People & Culture • Dept Heads & Senior Managers • Quality Improvement	Roles & Responsibilities • Board Secretary • People & Culture	Roles & Responsibilities • Board Secretary • People & Culture • Quality Improvement • Dept Heads & Senior Managers

GOVERNANCE

- **Board via Audit, Risk Management, & Compliance Committee**
- **Executive Leadership Team**
- **General Counsel & Board Secretary in role of Privacy Officer**
- **Departmental Heads & Senior Managers**

The Privacy Framework is comprised of four elements:

- Compliance with privacy laws and privacy principles, and other relevant legislation
- Provision of advice and guidance internally and externally regarding privacy rights and responsibilities
- Training and awareness activities within the organisation
- Monitoring, reporting and managing privacy practice including incident management.

ESTA's privacy strategy is a dynamic action plan aimed at driving the delivery of each element in the framework. It is linked to ESTA's Risk Management Framework.

3.3 Roles and Responsibilities

3.1.1 Board / ARMCC

The Board via its Audit, Risk Management and Compliance Committee (ARMCC) oversees information privacy management and its effectiveness

3.1.2 CEO an Executive Leadership Team (ELT)

The ELT has overall responsibility for information privacy management at ESTA and drives a continuous improvement culture. This includes responsibility and oversight for the:

- Information privacy management functions
- Liaison between the ARMCC and ESTA

3.1.3 General Counsel and Board Secretary (Privacy Officer)

The General Counsel and Board Secretary, in the role of Privacy Officer, is responsible for the maintenance of this framework

3.1.4 Employees and Contractors

All ESTA managers, employees and contractors are responsible for:

- Complying with the secrecy provisions of the *Emergency Services Telecommunications Act 2004 (Vic)* (the ESTA Act)
- Complying with the *Privacy & Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)* as they apply to ESTA, including compliance with privacy principles
- Reporting privacy breaches when they become aware of them

- Participating in training and awareness activities provided by ESTA, and communicating areas for improvement.

4 Policy overview

This policy refers to the use and management of personal and health information collected by ESTA. Personal information and health information held by ESTA is managed in accordance with the privacy principles contained in the *Privacy & Data Protection Act 2014 (Vic)* (the Information Privacy Principles) and the *Health Records Act 2001 (Vic)* (the Health Privacy Principles) and, as required, by other legislative provisions.

Legislative provisions include the Secrecy provisions in the ESTA Act that apply to ESTA employees and others working in ESTA's call-taking and dispatch operations environment.

All ESTA employees and contractors are required to comply with this policy at all times. This includes during business hours, outside of business hours and/or during non-business related activities whether the individual is acting in their capacity as an employee or not, and to all personal and health information collected, used, stored, disclosed, presented or accessed in connection with the employee's involvement with ESTA.

This policy applies to all activities of ESTA where personal or health information is collected, used, stored, disclosed, presented or accessed. Personal and health information that ESTA deals with can include, but is not limited to:

- in the case of personal information, information about callers, patients, members and employees whose identity is apparent or can reasonably be ascertained from that information; and
- In the case of health information, information about the health, any injuries or disabilities to an individual, or information about health services provided or to be provided to the individual, where the individual's identity is apparent or can reasonably be ascertained from that information.

5 The legislative framework

5.1 Emergency Services Telecommunications Act 2004 (Vic)

ESTA is established under the ESTA Act, which makes provision for emergency services telecommunications services and other communications services to be provided by ESTA in Victoria.

Section 33 of the ESTA Act is titled "Secrecy" and protects the "confidential information" of callers (whether or not such information is considered personal or health information) by limiting the use that ESTA, its employees and any other person may make in relation to that information. Confidential information under the ESTA Act is:

> *…any information relating to calls received or messages communicated by [ESTA] in the course of providing a service to an emergency services and other related services organisation.*

The restriction on the use of confidential information is as follows:

> *A person who has confidential information that he or she has received in the course of carrying out duties under the ESTA Act must not, except to the extent necessary to perform duties under the ESTA Act, record, disclose, communicate or make use of that information.*

All ESTA employees are required to comply with this restriction. Penalties outlined in the ESTA Act may apply for proven breaches of this restriction. Internal disciplinary action may also apply for breaches including dismissal.

This restriction does not, however, prevent a person (including ESTA and any ESTA employee) from:

- Giving evidence or producing documents in court in the course of criminal proceedings;
- Disclosing or communicating confidential information with the written authority of the responsible Minister, or of the person to whom the information relates;
- Disclosing or communicating confidential information to the Victorian Ombudsman or the Ombudsman's officers, or otherwise disclosing confidential information where specifically authorised under another Act;
- Disclosing confidential information to the extent specifically authorised by another Act.

Any reliance on the above exceptions by an ESTA employee must be approved by ESTA's Privacy Officer (or his/her authorised nominee).

A full extract of Section 33 of the ESTA Act is provided at Appendix A.

5.2 Ministerial Authorisation

The ESTA Act permits disclosure of confidential information with the written authority of the Minister.

ESTA has Ministerial Authorisation permitting the release of otherwise confidential information in specific circumstances. These include for the purposes of:

a. educating the community or any section of the community about the role of, and the services offered by, the Authority;

b. promoting public health and safety;

c. responding to complaints, enquiries or compliments about or relating to the Authority, a member of or acting member of the Authority or an employee of the Authority;

d. support for the employees of the Authority, which may include commendations or other recognition;

e. responding to requests for access to records under the *Freedom of Information Act 1982 (Vic)* so far as the exemptions contained in that Act (other than that contained in section 38 of that Act) do not apply to the information.

The Authorisation does not permit the disclosure or communication of information that would reveal the identity of an individual or an organisation without the express or implied consent of each individual or organisation concerned. If an individual is incapable of giving consent, the consent of the individual's next of kin or personal legal representative must be obtained.

An audio recording of a call may only be disclosed or communicated to a party to the call; or for a purpose set out in clauses (a), (b) and (d) above.

The Ministerial Authorisation restricts who from ESTA may permit the release of call audio and similar personal information.

A copy of the Ministerial Authorisation is available from ESTA's Privacy Officer.

5.3 Privacy and Data Protection Act 2014 (Vic) and Health Records Act 2001 (Vic)

ESTA is also bound by the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001 (Vic)* in relation to the handling of personal and health information.

The *Privacy and Data Protection Act 2014 (Vic)* regulates the collection and handling of personal information in the Victorian public sector. Under the *Privacy and Data Protection Act 2014 (Vic)*, ESTA is required to handle personal information (excluding any health information, which is regulated under the *Health Records Act 2001 (Vic)*) in accordance with the Information Privacy Principles (IPPs). The IPPs also apply to ESTA's handling of employee information.

The *Health Records Act 2001 (Vic)* regulates the handling of health information by Victorian public and private sector bodies holding health information. Under the *Health Records Act 2001 (Vic)*, ESTA is required to handle health information in accordance with the Health Privacy Principles (HPPs). The *Health Records Act 2001 (Vic)* also provides individuals with a right of access to their health information, however for ESTA, this right is superseded by rights provided to those individuals under the FOI Act and/or Ministerial Authorisation.

Health information is more fully described in the Definitions section of this Policy, but includes personal information about the physical, mental or psychological health or disability about an individual and the health services provided to him or her.

In addition to the use and disclosure of personal information for the primary purpose for which it was collected, both the Health Records Act and the Privacy and Data Protection Act allow for use and disclosure of information:

- Where required or authorised under law (such as under the ESTA Act); or
- If the use or disclosure it is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare.

While the two sets of privacy principles and health privacy principles are similar, they are not identical. A summary of the information and health privacy principles is provided at Appendix B.

Given the context of the services that ESTA provides to ESOs under the ESTA Act, and the highly critical nature of ESTA's operations, ESTA is generally permitted to collect and disclose personal and health information to ESOs and others in the performance of its services. In addition to this, the section 33(2) of the ESTA Act permits disclosure of confidential information to the extent such disclosure is necessary to perform duties under the Act.

However, the collection and disclosure of personal and health information by ESTA continues to occur within the context of the ESTA Act, the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)*, including in compliance with the IPPs and HPPs as they apply to ESTA. ESTA continues to take reasonable steps to manage inherent risk in respect of personal and health information.

The following sections outline the way in which ESTA will ensure it meets the key requirements of the information and health privacy principles.

6 Collection of Information

ESTA only collects information necessary to provide the Victorian community with its services, which is the provision of services in the nature of emergency telecommunications and other telecommunications services to emergency services and other related services organisations, as permitted under the ESTA Act.

Personal and/or health information is also collected:

- If an individual has applied for employment with ESTA;
- As part of an individual's employment with ESTA (e.g. administration of policies relating to employees, contact details);
- When individuals call triple zero and ESTA communications centres, by their voice being recorded (and caller line identification is used to determine the billing address of the caller); and

- From callers and emergency services organisation about third parties such as those requiring emergency assistance.

ESTA will collect non-identified information wherever practicable, in accordance with the information and health privacy principles.

When collecting personal or health information from an individual, reasonable steps must be taken by ESTA to ensure that the individual is aware of the following matters:

- What the information will be used for;
- Who the information is likely to be disclosed to and how it will be stored;
- Any law requiring the information to be collected;
- The main consequences if the information is not provided; and
- The individual's rights to access the information.

6.1 Sensitive information (IPP 10)

ESTA will only collect, use or disclose sensitive information where the individual has consented, the collection, use or disclosure is required under law, or is otherwise necessary to prevent or lessen a serious and imminent threat to the life or health of an individual and the individual is incapable of giving or communicating consent. See Appendix B for more information regarding IPP 10 Sensitive information.

7 Use of Information

ESTA may use information about an individual for the primary purpose for which the information was collected, as specified below, or a secondary purpose that is related to the primary purpose that a person would reasonably expect. If the use is not related to the primary purpose of collection the individual must generally consent to that use.

ESTA uses personal or health information that has been collected, for the purpose for which that information was collected by ESTA. This includes therefore the provision of personal and health information to ESOs in relation to the provision of call taking and dispatch services, and operational communications services, to those ESOs and, in the case of employees, administering ESTA's operational and human resources functions.

Stringent steps are to be taken to ensure the confidentiality, integrity and availability of personal information. Personal and health information may be collected for any of the following purposes:

- To establish the purpose of the call and/or the nature of the emergency
- To dispatch an ESO resource
- To provide pre-arrival instructions
- To assist in further training (note: wherever possible personal or health information is de-identified when used for this purpose, unless this use can be considered a secondary purpose related, or for health information directly related, to the primary purpose, and for which the individual would reasonably expect the information to be used)
- Audit and review purposes
- To process an application for employment with ESTA, including referee and police checks
- To efficiently manage the employment, salary, conditions of employment, workers compensation and other insurance claims of ESTA employees, including the provision of peer support services and welfare services for employees.

Occasionally, ESTA may be required or authorised by law (for example under the ESTA Act, the Privacy and Data Protection Act, the Health Records Act and other legislation applicable to ESTA) to use or provide personal or health information to others for limited purposes.

In other cases, where the use or disclosure is not otherwise permitted under this framework and the IPPs or HPPs (as applicable), ESTA will seek an individual's consent to use or provide that personal or health information to others.

8 Disclosure of Information

ESTA may disclose information about an individual for the primary purpose for which the information was collected, as specified above at section 6, or a secondary purpose that is related to the primary purpose that a person would reasonably expect. If the disclosure is not related to the primary purpose of collection the individual must generally consent to that disclosure.

Personal or health information may be provided to organisations that assist ESTA in providing a service to customers. Where ESTA has a contractual relationship with such third parties, ESTA should endeavour to include privacy provisions in the contract to impose the obligations under the information and health privacy principles on that third party as a contracted service provider. Where ESTA is outsourcing services to a service provider under such an agreement, the service provider will be bound by the information and health privacy principles (as applicable), for its own acts or practices. However, where the agreement with a service provider does not include the appropriate legal provisions, both ESTA and the service provider may be found liable for the service provider's acts or practices in breach of the information and health privacy principles. ESTA may also provide personal or health information to the following third party organisations:

- To an emergency services agency
- To other organisations where that organisation is responsible for payment of compensation (for example, the Transport Accident Commission, Victorian Workcover Authority)
- In dealing with prospective employees (for example, in relation to reference checks)
- In dealing with current employees (for example, in relation to the employees' superannuation fund).

These organisations will each continue to treat the personal or health information in accordance with the information and health privacy principles.

Both the Health Records Act and the Privacy and Data Protection Act allow for use and disclosure of information:

- Where required or authorised under law (such as under the ESTA Act)
- If the use or disclosure it is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare.

8.1 Transmission of information

ESTA limits radio and pager service transmission of information to that required by the relevant emergency services agency and in line with agreed communications standing operating procedures.

9 Data quality, security and retention

All stored personal and health information will be protected from unauthorised access, misuse, modification, loss or disclosure in accordance with the information and health privacy principles through the use of appropriate security and storage arrangements. ESTA will take reasonable steps to ensure that personal and health information that it holds is accurate, complete, up to date and relevant to the functions it performs.

Where personal or health information is used for audit or educational purposes, that information, and any other data provided for those purposes will be suitably protected.

9.1 Trans-border data flows

ESTA will not disclose or otherwise transfer any personal or health information in the performance of its services to any person (other than itself) who is outside Victoria unless permitted under this framework and the information and health privacy principles, and

- ESTA reasonably believes that the recipient is subject to a law, binding scheme or contract which is substantially similar to the information and health privacy principles;
- The individual has consented;
- The transfer is necessary for the implementation of pre-contractual measures, the performance or the conclusion of a contract with the individual or in the individual's interest;
- The contract is for the individual's benefit, it is impracticable to obtain consent to the transfer and the individual would be reasonably likely to give that consent;
- ESTA has taken reasonable steps to ensure the information will not be held, used or disclosed inconsistently with the information and health privacy principles; or
- The transfer is required or authorised by law;
- If the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare.

ESTA does take some calls for assistance from outside State boundaries and liaises with emergency services from other states, and Victorian emergency services operating across state borders.

10 Relationship between Privacy and Release of Information

10.1 Access to and correction of information

Individuals have a right to seek access to their own health information held by an organisation and to correct that information if it is inaccurate, incomplete, misleading or not up to-date. An organisation may only refuse in limited circumstances that are detailed in the Health Records Act, for example where disclosure might threaten someone's safety.

In the event that information being requested falls into the categories of documents that are subject to the FOI Act, the procedures for access or correction are those under the *Freedom of Information Act 1982* (FOI Act). Given that the FOI Act applies to ESTA and documentation that it holds, where a person requests access to or correction of a document from ESTA, the request will be reviewed and addressed in one of two ways:

- Under Ministerial Authorisation as set out in s33 of the ESTA Act and outlined at section 5.2 of this policy
- Under ESTA's FOI procedures in accordance with the FOI Act.

10.2 Freedom of Information Act 1982 (Vic)

The FOI Act applies to Victorian government agencies, which includes government departments, councils and prescribed authorities such as ESTA. The objective of the FOI Act is to extend, as far as possible, the right of the community to access information in the possession of the Government of Victoria.

Section 13 of the FOI Act creates a general right of access to documents in the possession of an agency. It provides that every person has a legally enforceable right to obtain access to documents of an agency, other than exempt documents. There are a number of categories of exempt documents outlined in the FOI Act.

Whether a person has a right of access to a document largely depends on whether the document is held by an agency such as ESTA; and is not an exempt document. Finally, the concept of a document under the FOI Act is a broad one. It extends beyond written documents to include (among others) CAD data, computer files and audio recordings.

ESTA is ordinarily obliged to process requests for documents sought under the FOI Act, if those documents are in its possession at the time of the FOI request. However, recordings and transcripts of triple zero calls recorded by ESTA, and event chronologies created by ESTA, while in ESTA's possession, are likely to be considered exempt documents for one of the following reasons:

- A secrecy provision applies to such documents (FOI Act, s 38, on the basis that the secrecy provision in ESTA Act, s 33(2) applies); and/or
- Release of such documents may affect personal privacy, involving an unreasonable disclosure of the affairs of a person other than the FOI applicant (FOI Act, s 33(1)).

FOI requests may be made via the Board Secretary.

11 Conformance

ESTA will treat any non-conformance with or breach of this policy as a serious issue. ESTA employees must comply with this policy and relevant legislation at all times, and where they do not, non-conformance or breach may result in disciplinary proceedings, including and up to dismissal.

Breaches of the secrecy provisions of the ESTA Act by any person may also result in a penalty being imposed on that person under the ESTA Act. Breaches of the Health Records Act also carry significant penalties.

Breach of the IPPs and/or the HPPs may result in an investigation of ESTA by the Commissioner for Privacy and Data Protection or the Office of the Health Services Commissioner, or the issue of compliance notices and/or monetary penalties imposed upon ESTA.
Privacy related complaints may be reported to the Privacy Officer via email at privacy@esta.vic.gov.au. More detailed information regarding breach management is outlined in ESTA's Privacy Procedures.

12 Definitions

Term	Definition
CTD	Call-taking and Dispatch
Emergency telecommunications and other telecommunications services	Either or both of the following: (a) call taking and dispatch services and (b) operational communications services
ESO	Emergency Services Organisation
ESTA	Emergency Services Telecommunications Authority
ESTA Act	*Emergency Services Telecommunications Authority Act 2004* (Vic)

FOI Act	*Freedom of Information Act 1982* (Vic)
Health information	Health information under the *Health Records Act 2001* (Vic), which includes information or an opinion about: (a) the physical, mental or psychological health (at any time) of an individual (b) a disability (at any time) of an individual (c) an individual's expressed wishes about the future provision of health services to him or her; or (d) a health service provided, or to be provided, to an individual, that is also **personal information** (but excluding information about an individual who has been dead for more than 30 years). Health information also includes any other health information under the *Health Records Act 2001* (Vic) such as additional information regarding organ donations and genetic information.
Health Privacy Principles or HPPs	Health Privacy Principles under the *Health Records Act 2001* (Vic).
Health Records Act	*Health Records Act 2001* (Vic).
Information privacy	The right of an individual to control the dissemination of personally identifying information about themselves.
Information Privacy Principles or IPPs	Information Privacy Principles under the *Privacy and Data Protection Act 2014* (Vic).
Non-identified information	Information or an opinion which is not personal information or health information, and from which the identity of an individual is not apparent and cannot reasonably be ascertained.
Personal information	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.
Privacy and Data Protection Act	*Privacy and Data Protection Act 2014* (Vic)
Sensitive information	Information or an opinion about an individual's (a)racial or ethnic origin; (b) political opinions; (c)membership of a political association; (d) religious beliefs or affiliations; (e) philosophical beliefs; (f) membership of a professional or trade association; (g) membership of a trade union; (h) sexual preferences or practices; or (i) criminal record that is also **personal information**.

APPENDIX A: Section 33 of the ESTA Act

Part 5 — General

33 Secrecy

(1) In this section ***confidential information*** means any information relating to calls received or messages communicated by the Authority in the course of providing a service to an emergency services and other related services organisation.

(2) A person who has confidential information that he or she has received in the course of carrying out duties under this Act must not, except to the extent necessary to perform duties under this Act, record, disclose, communicate or make use of that information.

Penalty: 5 penalty units.

(3) Subsection (2) does not prevent a person from—

(a) giving evidence or producing a document to a court in the course of criminal proceedings or proceedings under this Act, even though the evidence or document contains confidential information; or

(b) disclosing or communicating confidential information in accordance with the written authority of the Minister or the person to whom the information relates; or

(c) disclosing or communicating confidential information to an Ombudsman officer (within the meaning of the **Ombudsman Act 1973**); or

(d) disclosing confidential information to the extent specifically authorised by another Act.

APPENDIX B: Summary of Privacy Principles

This table sets out a summary version of the key privacy principles from the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*, as set out in those Acts and published by the Office of the Victorian Information Commissioner and the Victorian Health Complaints Commissioner, respectively.

These do not set out the full set or form of the relevant principles, and are intended for quick reference only. The principles in full can be found in the respective Acts or on the websites of the responsible Commissioners:

- Office of Victorian Information Commissioner
- Health Complaints Commissioner

Health Privacy Principles (HPPs) summary	**Information Privacy Principles (IPPs) summary**
1. Collection Only collect health information if necessary for the performance of a function or activity and with consent (or if it otherwise falls within the limited exceptions in HPP 1). Organisations must notify individuals about what the organisation will do with the information and that they individual can gain access to that information.	**1. Collection** An organisation can only collect personal information if it is necessary to fulfil its functions. It must collect information only by lawful and fair means and not in an unreasonably intrusive way. It must provide notice of the collection, including such things as the purpose of collection and how you can access the information.
2. Use and Disclosure Health information can only be used and disclosed for the primary purpose for which it was collected, for a directly related secondary purpose that the individual would reasonably expect or in other limited circumstances. Consent is required for other secondary uses except for some exceptions, such as law enforcement purposes and to protect safety.	**2. Use and Disclosure** Personal information can only be used and disclosed for the primary purpose for which it was collected, for a related secondary purpose that the individual would reasonably expect or in other limited circumstances. Consent is required for other secondary uses except for some exceptions, such as law enforcement purposes and to protect safety.
3. Data Quality An organisation must take reasonable steps to ensure health information you hold is accurate, complete, up-to-date and relevant to the functions it performs.	**3. Data Quality** An organisation must ensure personal information is accurate, complete and up-to-date.
4. Data Security and Retention An organisation must take reasonable steps to safeguard health information that it holds against misuse, loss, or unauthorised access, modification or disclosure. A health service provider must only destroy or delete health information as permitted under HPP 4, and any other organisation must take reasonable steps to	**4. Data Security** Personal information must be protected from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.

destroy or permanently de-identify personal information when it is no longer needed.	
5. Openness Organisations must have clearly expressed policies on the way they manage personal information. The organisation must make its privacy policy available to anyone who asks for it.	**5. Openness** Organisations must have clearly expressed policies on the way they manage personal information. The organisation must make its privacy policy available to anyone who asks for it.
6. Access and Correction Individuals have a right to seek access to their own health information held by an organisation and to correct that information if it is inaccurate, incomplete, misleading or not up to-date. An organisation may only refuse in limited circumstances that are detailed in the Health Records Act, for example where disclosure might threaten someone's safety. ***Note:*** *where the FOI Act applies to a document, this principle will not apply, and the FOI Act will apply, to access or correction of information in that document.*	**6. Access and Correction** Individuals have a right to seek access to their own personal information and to make corrections if necessary. An organisation may only refuse in limited circumstances that are detailed in the Privacy and Data Protection Act, for example where disclosure might threaten someone's safety. ***Note:*** *where the FOI Act applies to a document, this principle will not apply, and the FOI Act will apply, to access or correction of information in that document.*
7. Identifiers Organisations must only assign an identifier (i.e. a number or other identifier that is assigned to an individual in relation to their health information) to a person if the assignment is reasonably necessary to carry out its functions efficiently. A private sector organisation may only use or adopt an identifier assigned by a public sector organisation where the individual has consented, the use or disclosure is required or authorised by law, or necessary to fulfil its obligations to, or requirements of, the public sector organisation. ***Note:*** *example of an identifier includes a Medicare Number.*	**7. Unique Identifiers** Unique identifiers (i.e. a number or other identifier that is assigned to an individual for the purposes of an organisation's operations) can facilitate data matching. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions that are detailed in the Privacy and Data Protection Act, on how organisations use unique identifiers assigned by other organisations. Unique identifiers exclude identifiers as defined under the Health Records Act. ***Note:*** *examples of unique identifiers include Tax File Numbers or Driver's Licence Numbers.*
8. Anonymity Where lawful and practicable, an individual should have the option of transacting with an organisation without identifying him or herself.	**8. Anonymity** Where lawful and feasible, an individual should have the option of transacting with an organisation without identifying him or herself.
9. Transborder Data Flows If an individual's health information travels, that individual's privacy protection should travel with it.	**9. Trans-border Data Flows** If an individual's personal information travels, that individual's privacy protection should travel with it.

Transfer of health information outside Victoria is restricted, unless it is done so under one of the exceptions in HPP 9. Health information may be transferred only if the recipient protects privacy under standards similar to the Victorian HPPs.	Transfer of personal information outside Victoria is restricted, unless it is done so under one of the exceptions in IPP 9. Personal information may be transferred only if the recipient protects privacy under standards similar to the Victorian IPPs.
10. Transfer/closure of practice of health service provider Where the practice or business of a health service provider is to be sold, transferred or closed down, the health service provider must comply with this HPP in relation to notifying individuals and complying with individuals' requests to transfer information.	**10. Sensitive Information** The Privacy and Data Protection Act puts special restrictions on the collection of sensitive information. This includes an individual's racial or ethnic origin, political opinions and membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record.
11. Making information available to another health service provider If an organisation is a health service provider, it must make health information relating to an individual available to another health service provider if requested by the individual.	
Health Complaints Commissioner Level 26, 570 Bourke Street Melbourne Victoria 3000 Telephone: 1300 582 113 Website: https://hcc.vic.gov.au/contact	OVIC Office of the Victorian Information Commissioner Post: PO Box 24274 Melbourne VIC 3001 Telephone: 1300 006 842 Website: https://www.ovic.vic.gov.au/