Sexual Health Victoria

Care
Education
Advocacy

Privacy Policy

Sexual Health Victoria | 901 Whitehorse Road | PO Box 1377 | Box Hill Victoria 3128 | T/ 03 9257 0100 | F/ 03 9257 0112 ABN 97 379 402 182

1. PURPOSE

The purpose of this privacy policy is to outline the practices adopted by Sexual Health Victoria (SHV) for the management of personal and health information. It is designed to give individuals an understanding of the types of personal information SHV collects, and how it is used, stored, disclosed and able to be accessed.

The policy also outlines how individuals can correct their personal information, which is held by SHV, how to make a complaint about a breach of privacy, and how complaints will be handled.

Individuals who wish to contact SHV about information privacy or their personal information can do so by contacting the Privacy Officer at:

Email: privacyofficer@shvic.org.au
Telephone: 03 9257 0128
Mail: P.O. Box 1377 Box Hill VIC 3128

SHV is required to make this policy freely available and in an appropriate form, and accordingly it can be accessed on our public website. Individuals who would like to request a copy of this policy in an alternate form, for example suitable for the vision impaired, or individuals from a non-English speaking background, may do so by contacting our Privacy Officer, and reasonable steps in the circumstances will be taken to provide the policy in an appropriate form.

2. LEGISLATION

SHV is required to meet certain obligations under the Commonwealth Privacy Act 1988 (the Act) and is bound by the Australian Privacy Principles (the APPs) as well as the Victorian Health Records Information Act 2001. The Acts govern how SHV collects, uses, stores and discloses the personal information of individuals, and how they may access or correct their information.

Personal information broadly means information or an opinion about an individual, whether true or not, which could reasonably lead to the identification of the individual in the circumstances. Personal information can include name or address details, dates of birth, telephone numbers, email addresses, financial information such as banking details, or photographic or video material. An individual's name does not have to be included in information for it to constitute personal information. The test is whether the information considered as a whole would enable the individual to be identified.

A special category of personal information is known as "sensitive information", and can include information about race or ethnicity, political opinions or membership, religious or philosophical beliefs, professional or trade association or union membership, sexual preferences or practices, criminal records, health information and genetic/biometric information such as fingerprints. There are additional obligations for the management of sensitive information required by the Act.

Health information means information or an opinion about the health or a disability (at any time) of an individual; 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; 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 genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

3. WHAT KIND OF INFORMATION DO WE COLLECT AND HOLD?

SHV collects the personal information of clients, their representatives and next of kin, employees, members of the public and donors, suppliers, contractors and service providers. The personal information collected will depend on the nature of the individual's relationship or interaction with SHV and its staff. SHV will only collect personal information where it is reasonably necessary for, or directly related to, one or more of its functions or activities.

Personal information collected can include names, dates of birth, gender details, address and contact details including email addresses, belonging to our clients, next of kin and other legal representatives. Personal and business details of suppliers and contractors are also collected.

Additional personal information concerning employees which is collected can include job applications, work histories, resumes, educational qualifications, training records, competency assessments, details of salary and wages, training records, performance assessments, counselling details and personnel records. Sensitive information is sometimes collected when appropriate, such as criminal record check details and relevant medical histories for employment purposes.

Health information collected can include incident and accident reports, first aid records, workers compensation claims and documents, rehabilitation and attendance records, medical or other health service provider records, medical histories and other assessments for insurance or employment purposes. We collect information about our clients' health and care needs and their medical history as it relates to the care and services we provide, information about our clients' cultural, religious, linguistic and social needs, information about our clients' interests, hobbies and community activities, and information any potential medical, social or workplace risks involved in providing care and services to the client. Information about third parties is sometimes collected in the context of insurance claims.

4. HOW DO WE COLLECT PERSONAL INFORMATION?

Clients
We usually collect personal information about our clients in the following ways:

- directly from the client and/or their representatives or next of kin
- from clients' health care providers and other persons/organisations who provide care and services to the client
- where relevant, we also collect information about our clients from other care providers and care referral services.

We also receive information from the Commonwealth Government regarding our clients' eligibility to pay certain fees and charges.

Employees and service providers
We collect information about our employees:

- directly from the employees
- through general background check processes such as criminal history checks
- from other sources such as referees and employment agencies.
- Information about suppliers, contractors and service providers and their employees is collected directly from our service providers.

SHV collects personal information by way of several channels or methods. Personal information can be collected when individuals telephone SHV or interact verbally, or make contact by mail or

email. It is also collected when individuals access our website or use it to communicate with us. In most cases SHV collects information directly from individuals, however where information about you is collected from another person or organisation, it is dealt with according to the requirements of the Act.

Personal information can be collected when individuals use our online "contact us" form, or make enquiries or complaints. It is sometimes collected whether it has been requested by SHV or not, for example when you send us your personal information without us asking for it. Our website uses "Cookies" which collect user information and data for statistical and analytic purposes.

Personal and business details of suppliers, contractors and service providers are collected when they interact with SHV, so that appropriate financial and business records can be maintained. Personal information of job applicants and employees is also collected during the application process (whether or not successful) and during the period of employment, which may also include sensitive information. Health information can be collected when circumstances require that first aid be administered, for administering sick leave or carers leave, or where injury or insurance claims arise.

When personal information is collected, SHV takes reasonable steps in the circumstances to notify the individual (either at or before the time of collection, or as soon as practicable thereafter) or make them aware of certain matters. These "collection statements" are included on all forms that SHV uses to collect personal information, displayed on our website at the point of collection, or relayed via telephone or in person when individuals provide their personal information to us.

SHV must notify you of its identity and contact details, where and in what circumstances your personal information may be collected from another source, whether the collection is required or authorised by law or a Court/Tribunal order, the purposes for which it is collected, the main consequences if some or all of the information is not collected, and to whom the personal information is usually disclosed. SHV must also inform you that its Privacy Policy contains information about how to access and seek correction of personal information, how to make a complaint about a privacy breach, and how complaints will be handled. You must also be informed whether your personal information is likely to be disclosed to overseas recipients, and if it is practicable to do so in which countries they are located.

SHV is required to use its best endeavours to offer individuals the option of not identifying themselves, or using a pseudonym, when they interact with us. This requirement does not apply if we are required by law or authorised by a Court or Tribunal to only deal with individuals who have identified themselves, or where it is impracticable to deal with individuals in this manner.

5. HOW DO WE STORE PERSONAL INFORMATION?

SHV stores information securely both in paper form and electronically at its head office. Authorised staff providing care and services have access to personal and health information electronically and in paper format.

SHV is required to take reasonable steps to ensure that the personal information it collects, holds, uses and discloses is accurate, up to date and complete, with reference to the purpose for which it is collected, used or disclosed. Information held by SHV is subject to regular reviews and audits for this purpose. Where it is determined that it is no longer necessary or legally required for SHV to hold and store personal information, reasonable steps are taken to de-identify or destroy the information.

SHV stores information using a combination of physical files and a secure electronic finance and HRI system for personnel and invoicing related records. Security and access protocols are maintained in order to implement reasonable steps to ensure that personal information is protected from misuse, interference, loss, unauthorised access, modification and disclosure. Internal access controls and protocols ensure that only authorised staff can access personal

information in circumstances where they are required to do so in the performance of their duties. Our IT system allows electronic file access to be tracked and audited to ensure that only authorised access to personal information has occurred.

Governance mechanisms employed by SHV to ensure the appropriate management of personal information include maintaining a designated privacy officer role, our internal policies and procedures, audit programs, staff communications and training programs. SHV is committed to conducting a Privacy Impact Assessment for any new project where personal information will be handled, or where a significant change to information handling procedures is proposed.

6. FOR WHAT PURPOSES DO WE COLLECT, HOLD, USE AND DISCLOSE PERSONAL INFORMATION?

Use of information
When SHV holds your personal information, it can only be used for the particular purpose for which it was collected (known as the "primary purpose"), unless certain exceptions apply. Personal information can be used for secondary or other purposes where consent has been obtained, where it is reasonably expected to be used for a related purpose, where required or authorised by law or a Court/Tribunal order, where reasonably necessary for enforcement purposes conducted by or on behalf of an enforcement body, or where certain "permitted general situations" or "permitted health situations" exist.

Permitted General Situations
Permitted general situations are where circumstances exist involving serious threats to life, health or safety of any individual, or to public health or safety, suspected unlawful activity or serious misconduct, missing persons, legal or equitable claims and alternative dispute resolution processes.

Permitted Health Situations
Permitted health situations are where a range of specific circumstances apply in relation to the collection, use and disclosure of health information. They will exist where the information is necessary to provide a health service to the individual, and either the collection is required or authorised by or under an Australian law (other than the Privacy Act), or the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which govern activities of the organisation.

A permitted health situation will also exist where the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- those purposes cannot be served by collecting de-identified information,
- it is impracticable to obtain the individual's consent, and
- the collection is either required by or under an Australian law (other than the Privacy Act), in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or in accordance with approved guidelines.

A further permitted health situation will exist if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual's consent to the use or disclosure,
- the use or disclosure is conducted in accordance with approved guidelines, and

- in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

Permitted health situations arise in relation to genetic information about an individual if:

- the organisation has obtained the information in the course of providing a health service to the individual,
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual,
- the use or disclosure is conducted in accordance with approved guidelines, and
- in the case of disclosure – the recipient of the information is a genetic relative of the individual.

Finally, a permitted health situation will arise when the organisation provides a health service to the individual, and:

- the recipient of the information is a responsible person for the individual,
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure,
- another individual providing the health service (the 'carer') is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons,
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware, and
- the disclosure is limited to the extent reasonable and necessary for providing appropriate care or fulfilling compassionate reasons.

SHV uses personal information provided during enquiry processes for the purposes of fulfilling client requests, providing personalised services, maintaining accounts and records, statistical analysis, conducting market research and marketing, and assessing and evaluating the use of our website. Personal information may also be used by SHV in conducting criminal record checking and employment screening, obtaining legal advice, and participating in legal proceedings.

7. DISCLOSURE OF OR ACCESS TO INFORMATION

In most circumstances, SHV is restricted in how it may disclose your personal information. Personal information can only be disclosed for the particular purpose for which it was collected (known as the "primary purpose"), unless certain exceptions apply. Personal information can be disclosed for secondary or other purposes where we have consent to do so, where it is reasonably expected to be disclosed for a related purpose, where required or authorised by law or a Court/Tribunal order, where reasonably necessary for enforcement purposes conducted by or on behalf of an enforcement body, or where "permitted general situations" or "permitted health situations" as described above exist.

Circumstances where personal information may be disclosed broadly include compliance with statutory obligations, arranging for insurance, progressing insurance claims and meeting occupational health and safety obligations. SHV may disclose personal information of members of the public, clients, suppliers, contractors and service providers which is provided for the

purposes of fulfilling client requests, providing personalised services, maintaining accounts and records, statistical analysis, conducting market research and marketing, and assessing and evaluating the use of our website.

Personal information may also be disclosed for residential application assessment, administration of resident agreements, and in some circumstances in obtaining references. Other circumstances where it may be disclosed include complaint management, security purposes, and administration of job applications and employment, which may include criminal record checking and employment screening. Personal information may also be disclosed by SHV in obtaining legal advice, and participating in legal proceedings.

Personal information may be given to State and Commonwealth government agencies and other individuals/organisations including loss adjusters, security companies, insurance companies and health service providers. It will only be disclosed to third parties where permitted by the Act, and only disclosed to SHV staff where necessary for the performance of their duties and where they are authorised to access it.

Clients
We collect, hold, use and disclose personal information about our clients for the primary purposes of providing care and services to our clients.

Where permissible, we disclose clients' relevant personal information other persons/organisations who are involved in providing health services and other care and services to the client. This can include the client's doctor and allied health service providers. It can also include people such as personal care workers.

We also collect, hold, use and disclose clients' information for the following purposes:

- so that we can receive funding from government agencies in respect of our clients
- so that we can improve our services through quality improvement activities such as audits, surveys and other quality improvement activities
- for direct marketing
- for the purposes of obtaining professional advice

Employees and service providers
We collect, hold, use and disclose information about our employees and services providers for following purposes:

- to administer employment arrangements, personnel development and management responsibilities
- to provide services to our clients
- for quality improvement and marketing purposes
- to meet our legal obligations such as the requirement to obtain criminal record checks for employees involved in providing care to our clients and workplace laws obligations.

8. DIRECT MARKETING

SHV may use or disclose personal information (other than sensitive information) for direct marketing purposes where it has collected the information directly from the individual, the individual would reasonably expect the information to be used for that purpose, where a simple means for the individual to opt out of direct marketing communications has been provided and where the individual has not done so.

Direct marketing can also occur where SHV has consent to use personal information for that purpose, whether or not the information was collected from the individual, where a simple means

for the individual to opt out of direct marketing communications has been provided with each direct marketing communication and where the individual has not done so.

SHV can use sensitive information for direct marketing communications where consent to do so has been obtained.

When SHV uses personal information for direct marketing purposes or to facilitate direct marketing by another organisation, the individual may request not to receive marketing communications, request that SHV not use or disclose their personal information to facilitate direct marketing by another organisation, and request that SHV inform the individual of the source of their personal information where practicable or reasonable (or inform the individual that it cannot do so).

SHV cannot charge an individual for dealing with a request not to receive direct marketing communication, that their information not be disclosed to another marketing organisation, or to provide its source of information. It must deal with these requests within a reasonable period of time and will usually do so within seven days.

9. HOW CAN YOU ACCESS AND CORRECT YOUR PERSONAL INFORMATION?

Access Requests
Requests made by individuals to access their personal information held by SHV will generally be granted unless certain limited circumstances apply. Those circumstances may include where it is reasonably determined that granting access would pose a serious threat to the life, health, or safety of an individual or to public health or safety, where granting access would have an unreasonable impact on the privacy of other individuals, where the request is frivolous or vexatious, or where legal proceedings are on foot. SHV may also deny access in some circumstances where it is required to do so by law or access would be unlawful, where commercial negotiations or decision-making processes may be prejudiced, where unlawful activity or serious misconduct is suspected, or where enforcement related activities may be prejudiced.

SHV responds to requests to access personal information within a reasonable period (usually 45 days but often sooner) and gives access to the information in the manner requested where it is reasonable and practicable. If access needs to be refused due to one of the above exceptions, SHV will take reasonable steps in the circumstances to provide access that meets the needs of SHV and the individual, including through using a mutually agreed intermediary.

If access is refused, SHV will give the individual a written notice which sets out the reasons for refusal, how to complain about the refusal, and where it relates to a commercially sensitive decision-making process, the reasons for refusal may include an explanation of the nature of the commercially sensitive decision.

SHV may require that reasonable charges be paid in respect of granting access to personal information, however the charges must not be excessive, and must not apply to the making of the request. Requests for access to personal information can be made by contacting our Privacy Officer directly.

Requests to update or correct
If SHV holds personal information about an individual, and is satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading (having regard to the purpose for which it is held), or the individual requests that SHV correct the information, then SHV will take reasonable steps to correct the information to ensure that it is accurate, up to date, complete, relevant and not misleading.

When SHV corrects personal information that it previously disclosed to someone else, and the individual requests that SHV notify the other person of the correction, then SHV will take

reasonable steps in the circumstances to give that notification unless it is impracticable or unlawful to do so. If in some circumstances SHV refuses to correct personal information as requested, it will provide the individual with a written notice that sets out the reasons for refusal, and how to complain about the refusal.

When SHV refuses to correct personal information as requested, and the individual requests SHV to add a statement to their record that the information is inaccurate, out of date, incomplete, irrelevant or misleading, then SHV will take reasonable steps in the circumstances to add the statement to the record in a manner that will make it apparent to users of the information. SHV will respond to requests to correct/update or add a statement within a reasonable period after the request is made and will not charge the individual for the making of the request, the correction, or the adding of the statement.

Requests to update or correct personal information can be made by contacting our Privacy Officer directly. Requests will usually be met or responded to within 30 days.

10. HOW CAN YOU COMPLAIN ABOUT A BREACH OF THE APPS?

All complaints concerning breaches of the Act and APPs will be examined, and unless they are considered frivolous or vexatious, will be investigated by SHV's Privacy Officer. Complaints should be submitted in writing directly to the Privacy Officer via the contact details on page 1 of this policy. SHV follows dedicated procedures for identifying and reporting privacy breaches, and for receiving and responding to complaints.

SHV's Privacy Officer maintains a complaint register and will investigate complaints concerning the mishandling of personal information, security breaches, and allegations of breaches of the Act and the APPs, and any matters which are referred from the Office of the Australian Information Commissioner (OAIC). Your complaint will be promptly acknowledged and will be dealt with within a reasonable amount of time depending on the complexity of the matter. You will receive updates as to the progress of your complaint if the investigation takes longer than expected. Less complex complaints can usually be dealt with within 30 days, however more complex matters may take longer to resolve.

Where a notification of a breach of privacy, or a complaint about the handling of personal information is received, SHV's Privacy Officer will take immediate steps to contain the breach, which may involve securing or quarantining personal information or SHV files which contain the personal information. A preliminary assessment will be conducted and any necessary actions taken. These actions may include notifying the individual(s) whose personal information is subject of the breach/complaint.

Where the preliminary assessment finds that the matter is complex or of a serious nature, independent investigators and/or legal advisors may be retained to assist with the investigation. All investigations will determine whether or not there appears to have been a breach of SHV's obligations under the Act. At the conclusion of the investigation, recommendations may be made as to changes to information handling practices and protocols within SHV. The complainant (or if the matter was referred by it, the OAIC) will be informed of the outcome of the investigation, any relevant findings, and any actions taken as a result.

If the complainant is not satisfied with the investigation or the outcome, they may make a further complaint to the Office of the Australian Information Commissioner.

Further information can be found at http://www.oaic.gov.au/privacy/making-a-privacy-complaint

11. DATA BREACHES

If there are any IT information breaches or the intentional or unintentional release of any personal information SHV contains such as (but not limited to):

- Tax File Numbers
- Any personal information
- Medicare information
- Student identification
- Health care records

The Data Breach Response Plan and Procedure will come into immediate effect in line with processes outlined by the Office of the Australian Information Commissioner (OAIC).

Document Control	
Approved by:	Chief Executive Officer
Responsible Program Area:	CEO Office
Approval Date	29 November 2019
Effective Date:	March 2015
Document Number:	PS-POL-035
Document Title:	Privacy Policy
Version:	5
Review Date:	November 2020