ACT Government | ACT Health

POLICY DOCUMENT

ACT Health Directorate Information Privacy Policy

Document number	AHDPD-24:2020
Effective date	3 January 2021
Review date	3 January 2024
Author branch	Information and Data Management Branch Digital Solutions Division
Endorsed by	Director-General
Audience	ACT Health Directorate – All Staff
Version number	1.0

Contents_Toc41813197

Policy Statement

ACT Health Directorate (ACT Health) is committed to ensuring information collected about an individual is managed in accordance with legislative requirements. ACT Health will not collect information if it is not required.

There are two types of information collected and managed by ACT Health whilst performing the functions of a health service organisation.

Any information collected by ACT Health in relation to the health, illness or disability of a consumer is personal health information. The management of this information is covered by the *Health Records (Privacy and Access) Act 1997* and *ACT Health Directorate Clinical Records Policy* and is out of scope for this policy.

Any other personal information collected by ACT Health, such as from an employee, volunteer, student, contractor or from a consumer through a consultation process is covered by the *Public Sector Act 2014*, *Information Privacy Act 2014*, and *Territory Records Act 2002*.

Purpose

The purpose of this policy is to set out how ACT Health collects, holds, uses and discloses personal information to carry out functions or activities, in accordance with the organisation's legal obligations under the *Information Privacy Act 2014*.

Scope

This policy applies to all people who work (paid and unpaid) at ACT Health. This includes but is not limited to, staff members, contractors, students, volunteers, seconded and outposted officers from other ACT Government entities who during their work have access to an individual's personal information. Throughout this document, all of these people who work (paid and unpaid) at ACT Health are referred to as staff.

This policy applies to all personal information (that does not form part of a clinical record), in any format, that is collected, held, used and disclosed by any part of ACT Health.

Personal health information and the management of clinical records is out of scope of this policy. These are covered by the *ACT Health Directorate Clinical Records Policy* and by the *Health Records (Privacy and Access) Act 1997*.

This policy does not provide detail about records management. Please see the *ACT Health Directorate Records Management Policy* and *Territory Records Act 2002* for further information in relation to administrative records management.

This policy does not provide detail about how to manage requests under the *Freedom of Information Act 2016*. Further information on Freedom of Information (FOI) is available on HealthHQ.

This policy does not provide guidance to assist in understanding points of contact and escalation processes when dealing with media communications and community engagement. These are outlined in the *ACTPS Media Communications and Engagement Policy*. The ACT Health Media Team (HealthMedia@act.gov.au / 0403 344 080) must be advised of all media contact.

Roles and Responsibilities

Position	Responsibility
Chief Information Officer/Executive Group Manager, Digital Solutions Division	Ensuring the organisation complies with this policy Ensuring the organisation meets the legislative requirements of the *Information Privacy Act 2014*.
Senior Executive Staff (ie EBMs, EGMs, DDGs and DG)	Ensuring staff are aware of the legislative requirements of the *Information Privacy Act 2014* Ensuring all staff are orientated to this policy and their associated responsibilities.
All Staff	Adhering to the Territory Privacy Principles of the *Information Privacy Act 2014.* Following this policy when managing personal information. Only accessing information needed to perform their duties. Protecting the privacy and confidentiality of personal information that they may collect or hold. Not disclosing personal information without legal authority. Accepting responsibility for all activities undertaken using their ICT access credentials and OneID access card. Not removing confidential information from the workplace unless authorised. Disposing of any documents with personal information, that are not required to be filed in an administrative record, into a secure waste bin.

Requirements

This policy outlines the standards that must be followed by ACT Health on how to manage personal information as outlined by the Territory Privacy Principles (TPP) of the *Information Privacy Act 2014*:

TPP 1 –	open and transparent management of personal information
TPP 2 –	anonymity and pseudonymity
TPP 3 –	collection of solicited personal information
TPP 4 –	dealing with unsolicited personal information
TPP 5 –	notification of the collection of personal information
TPP 6 –	use or disclosure of personal information
TPP 7 –	direct marketing (Commonwealth of Australia Act privacy requirement)
TPP 8 –	cross-border disclosure of personal information
TPP 7 –	adoption, use or disclosure of government-related identifiers (Commonwealth of Australia Act privacy requirement)
TPP 10 –	quality of personal information
TPP 11 –	security of personal information
TPP 12 –	access to personal information
TPP 13 -	correction of personal information

Collection of Personal Information

Remaining anonymous

Generally, when an individual communicates with staff (for example when calling on the phone to make an enquiry) they have the option of remaining anonymous or using a pseudonym (a made-up name).

However, in some situations it is impracticable or unlawful for staff to deal with an individual without them providing identifying information, such as collecting information from an individual regarding employment at ACT Health. In this instance the individual will need to provide their name in order to receive services or assistance.

Collection of personal information

At all times staff will only collect personal information where that information is reasonably necessary for, or directly related to its functions or activities. Staff must not collect personal information if it is not required.

ACT Health staff will not collect sensitive information (see definition of terms) without an individual's consent unless it is required or authorised by a law, or court or tribunal order, or is necessary to prevent a threat to the life, health or safety of one or more individuals, or to public health or safety.

How do staff collect personal information?

Staff must only collect information by lawful and fair means.

An individual's personal information may be collected in a variety of ways. This includes paper or online forms, in correspondence to and from the individual as well as email, in person, over the telephone and by fax.

Staff collect personal information such as contact details and complaint, review, request or report details when:

- The organisation is required or authorised by law or a Court or tribunal order to collect the information. Any information that goes into a patient/consumer clinical record is personal health information and is not covered by this policy.
- The individual participates in community consultations, forums or make submissions to ACT Health, and consents to the organisation's collection of their personal information.
- The individual contacts staff to ask for information (but only if staff need it to verify or follow up on the request).
- The individual makes a complaint about the way ACT Health have handled a Freedom of Information (FOI) request or seeks a review of an FOI decision.
- The individual applies for employment or is an employee at ACT Health.
- The individual seeks to enter a non-public area of an ACT Health facility.
- The individual asks for access to information ACT Health holds about them (excluding personal health information, please see *ACT Health Directorate Clinical Records Policy*) or other information about the operation of ACT Health.

Staff may also collect contact details and other personal information if an individual is on the organisation's committees or participating in a meeting or consultation with ACT Health.

Normally staff collect information directly from individuals unless it is unreasonable or impracticable to do so. In certain circumstances, for example where it is required by law, staff may also obtain personal information collected by other Australian, state and territory government bodies or other organisations.

Staff may also collect personal information from publicly available sources where that may enable the organisation to perform its functions effectively.

Types of information ACT Health collect and hold

At all times staff should only collect the information required to provide a service or response to the individual. The personal information staff collect and hold at ACT Health includes:

- Information about an individual's identity (e.g. date of birth, country of birth, passport details, photograph, visa details and drivers' licence)
- An individual's name, address and contact details (e.g. phone, email and fax)
- Information about an individual's personal circumstances (e.g. age, gender, marital status and occupation)
- Information about an individual's financial affairs (e.g. payment details, bank account details, and information about business and financial interests)
- Information about an individual's employment (e.g. applications for employment, work history, referee comments and remuneration)
- Information about assistance provided to an individual under the organisation's assistance arrangements.

Sensitive information is handled with additional protections under the *Information Privacy Act 2014*.

Notice of collection

When staff need to collect personal information from an individual, they are required to notify them about:

- Who ACT Health is and how ACT Health may be contacted.
- The circumstances in which ACT Health may or have collected personal information.
- The name of the law that requires ACT Health to collect this information (if any).
- The purposes for which ACT Health collects the information.
- How the individual may be affected if ACT Health cannot collect the information it needs.
- The details of any agencies or types of agencies which ACT Health normally share personal information with. This includes whether those recipients are overseas, and which countries those recipients are located in.
- That ACT Health have this policy to explain how the organisation handles individuals' information and deals with related complaints. A copy of the privacy policy can be provided to the individual or can be accessed via the ACT Health website.

Collection through ACT Health websites

Personal information collected through the ACT Health websites and affiliated applications is covered by the *ACT Government Web Privacy Policy* which can be viewed at https://www.cmtedd.act.gov.au/legal/privacy.

Social networking services

If an individual interacts with an ACT Health social networking page or profile, ACT Health has viewing access to the extent the individual's own privacy settings or disclosures allow. No personal information is collected or stored by ACT Health through its use of social networking services. Each social network (e.g. Facebook, Twitter) may collect information in accordance with its own privacy policies.

Email lists

ACT Health may use subscriber email lists to share information. On voluntarily subscribing, an individual's name and email address is collected and stored by ACT Health. An email with a link to unsubscribe is normally automatically emailed to individuals upon subscription. If it is not, or an individual has lost that email, they can reply to any subsequent email or click on a link in any subsequent email to request that they be unsubscribed from the distribution list.

Use and Disclosure of Personal Information

Staff must not use an individual's personal information for a secondary purpose or share their personal information without their consent, unless an exception/s applies under the *Information Privacy Act 2014, Territory Privacy Principle 6*. If such an exception applies ACT Health may use or disclose personal information for a secondary purpose consistent with those exceptions.

Exceptions are available in a number of circumstances including when:

- An individual would reasonably expect staff to use the information for the secondary purpose that is related (or directly related – in the case of sensitive information) to the original purpose for which the information was collected.
- The use or sharing of information is legally required or authorised by an Australian law, or court or tribunal order.
- The collection is reasonably necessary for a law enforcement-related activity. Such activity includes the prevention, detection, investigation, prosecution or punishment or criminal offences or breaches of the law; intelligence gathering, surveillance, conduct of protective or custodial services.
- Staff reasonably believe that collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- Staff have reason to suspect unlawful activity or serious misconduct that relates to its functions, and reasonably believe that collection of the information is necessary to take appropriate action.
- Staff reasonably believe that the collection is necessary to help locate a person who has been reported as missing.

If staff have collected and hold an individual's biometric information (such as their fingerprints or photograph) or biometric templates (digital representations of an individual's distinct characteristics) this information is allowed to be provided to other Canberra Health Services, Calvary Public Hospital Bruce OR an enforcement body (like the Australian Federal Police or Department of Home Affairs) in accordance with any guidelines made by the Office of the Australian Information Commissioner (OAIC).

Staff may also disclose personal information to Commonwealth intelligence agencies where this is authorised by the head of the intelligence agency and the agency certifies that the disclosure is necessary for its functions.

Reference should be made to the exceptions on use and disclosure available under *Information Privacy Act 2014, Territory Privacy Principle 6* and that ACT Health would use or disclose personal information for a secondary purpose consistent with those exceptions.

Sharing information with service providers

In some instances, ACT Health contracts with service providers to support ACT Health to carry out specific activities and functions. It may be necessary for staff to share personal information with these service providers to enable them to perform their functions.

In these situations, ACT Health protects personal information by only entering into contracts with service providers who agree to comply with Territory requirements for the protection of personal information.

Sharing information with other ACT Government entities

In some instances, ACT Health works with other ACT Government entities (such as Canberra Health Services, Access Canberra and Shared Services) to support ACT Health to carry out specific activities and functions. It may be necessary for staff to share personal information with these entities to enable them to perform their functions.

In these situations, ACT Health protects personal information as these ACT Government entities are bound by the same legislative obligations as ACT Health in relation to Territory requirements for the protection of personal information.

Disclosure of personal information overseas

In some circumstances ACT Health may need to share or store information with overseas recipients. Recipients may be located in any country.

Before releasing necessary personal information, staff will take reasonable steps to ensure that the recipient treats it with the standard of care required by the *Information Privacy Act 2014*.

In some cases, information will already be sufficiently protected under the law governing the overseas recipient, and the individual can access mechanisms to enforce those protections.

If it is practical and reasonable to do so, staff will obtain an individual's consent to overseas disclosure and notify them of the recipient's location. However, there may be situations where staff are unable, for example, where it shares information as part of a law enforcement activity.

For more information about use and disclosure of employee personal information please contact ACT Health People Strategy at HDHR@act.gov.au or call +61 2 5124 9201.

Quality of Personal Information

ACT Health must take reasonable steps to make sure the personal information it collects is accurate, up-to-date, and complete. Personal information ACT Health uses or discloses must also be relevant for the purpose for which it uses or discloses it.

Correcting personal information

If staff are satisfied that the personal information held about an individual is incorrect, inaccurate, incomplete, irrelevant, out-of-date or misleading, or an individual asks staff to correct their personal information, staff must take reasonable steps to correct information.

If staff agree to correct information previously shared with another agency, an individual may ask that staff notify the other agency of the possible need for correction.

There may be reasons why staff refuse or are unable to correct information, for example if it is impracticable or the organisation is required or authorised by law not to.

If staff refuse or are unable to correct the information, within 30 days ACT Health must give the individual written notice of why, and how the individual may complain about the decision.

If staff refuse or are unable to correct an individual's personal information, the individual can ask ACT Health to attach or link a statement to the information, stating that the individual believes the information is incorrect and why.

Staff will not charge an individual any fees for making the request for correction, correcting the information or attaching a statement to the personal information.

Storage and Security of Personal Information

ACT Health is required to take reasonable steps to make sure that personal information it holds is safe and secure.

ACT Health strives to protect personal information from misuse, interference or loss and from unauthorised access, use, modification or disclosure. This is in accordance with the *Information Privacy Act 2014*.

The *Territory Records Act 2002* establishes frameworks for the management of individuals' personal information. This includes personal information held within the files or data

systems provided by ACT Health. It also includes personal information held in paper based administrative records which are managed in accordance with the *ACT Health Directorate Records Management Policy*.

The organisation's Information Technology (IT) systems use comprehensive protections to guard against unauthorised access. Staff are responsible for complying with the *Information and Communication Technology Resources – Acceptable use* procedure. Data stored on mobile devices will be secured as per the *Mobile Communications Devices Management and Use Procedure.*

At ACT Health personal information is only available to staff who require access to perform their roles.

Accessing an individual's own personal information

In accordance with the *Information Privacy Act 2014* (Territory Privacy Principles 12 and 13) an individual has the right to ask for access to personal information that ACT Health holds about them. They are also entitled to request that staff correct that personal information, if they believe it is no longer accurate or up to date.

If an individual contacts staff to request access to their personal information staff must provide them with the following information:

- Employees wishing to access their personnel file can contact their manager.
- Other individuals wanting to access personal information not held in a clinical record can contact the Archives ACT Reference Archivist at reference@act.gov.au as per *ACT Health Directorate Records Management Policy*.

If the request to access information is not reasonable or practicable, staff must respond in writing within 30 days. This response must inform the individual why the organisation is unable to provide them with access to that information.

Individuals also have the right under the *Freedom of Information Act 2016* to request access to documents that ACT Health hold and ask that information be changed or annotated if it is incomplete, incorrect, out-of-date or misleading. Requests should be directed to HealthFOI@act.gov.au or +61 2 5124 9831.

How to make a complaint

Complaints about how ACT Health has managed an individual's personal information need to be made in writing. Staff can assist individuals to lodge their complaint if needed.

Individuals can contact the Chief Information Officer as the senior ACT Health officer responsible for Information Privacy via:

- Email – ACTHealthCIO@act.gov.au
- Telephone – +61 2 5124 9000
- Postal address – Office of the Chief Information Officer, ACT Health, GPO Box 825, Canberra ACT 2601

ACT Health will consider a complaint to work out how they can resolve the issue satisfactorily. ACT Health will advise individuals promptly that their complaint has been received and will respond within 30 days.

If an individual is not satisfied with the response, they may request a further response from the Office of the Chief Information Officer or can make a formal privacy complaint to the Office of the Australian Information Commissioner (OAIC). OAIC is an independent body that will assess the complaint. OAIC can determine that the actions of ACT Health are an interference with the individual's privacy. If the individual's complaint is upheld by the Commissioner, they may be able to seek a remedy in the Magistrates Court. OAIC can be contacted via:

- Email – enquiries@oaic.gov.au
- Telephone – 1300 363 992
- Postal address – GPO Box 5218, Sydney, NSW 2001
- Website – www.oaic.gov.au

Records Management

All Senior Executive Staff are responsible for determining the records required to demonstrate compliance with this policy for areas within their responsibility. At a minimum, this includes Standard Operating Procedures outlining Information Privacy steps, documentation of any collection, use, disclosure, sharing and correction of personal information. All records are to be maintained in accordance with the ACT Health Directorate Records Management Policy and Territory Records Act 2002.

The Chief Information Security Officer within the Digital Solutions Division is responsible for procedures and record-keeping in relation to storage and security of personal information across ACT Health.

Evaluation

Outcome Measures	Method	Responsibility
Compliance with this policy by ACT Health staff	**Annual survey to all ACT Health Senior Executives**	**Chief Information Officer**

References and Related Documents

Legislation

- *Freedom of Information Act 2016*
- *Health Records (Privacy and Access) Act 1997*
- *Human Rights Act 2004*
- *Information Privacy Act 2014*
- *Public Sector Act 2014*
- *Territory Records Act 2002*
- *Workplace Privacy Act 2011*

Supporting Documents

- *ACT Government Web Privacy Policy*
- *ACT Health Directorate Clinical Records Policy*
- *ACT Health Directorate Records Management Policy*
- *ACTPS Human resources privacy policy*
- *ACTPS Media Communications and Engagement*
- *ACTPS Use of Social Media Policy*
- *Information and Communication Technology Resources – Acceptable use*
- *Mobile Communication Devices Management and Use*

Definitions

Term	Definition
Personal Information	The *Information Privacy Act 2014* defines Personal Information as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.
Personal health information	The *Health Records (Privacy and Access) Act 1997* defines personal health information as any personal information, whether or not recorded in a health record, relating to the health, an illness or a disability of the consumer, or collected by a health service provider in relation to the health, an illness or a disability of the consumer.
Sensitive information	Information that is 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 orientation or practices
- Criminal record
- Genetic information
- Biometric information (including photographs, voice or video recordings).

Version Control

Version	Date	Comments
0.1	17 May 2020	Draft for consultation
0.2	31 May 2020	Final draft for consideration by Technology Strategy Committee and the Directorate Leadership Committee
1.0	3 January 2021	Final Version

Disclaimer: *This document has been developed by the ACT Health Directorate specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACT Health Directorate assumes no responsibility whatsoever.*