Policy No.: D0417

Workplace Surveillance Policy Directive

Version No.: 3.0
Approval date: 22 July 2019

Government of South Australia

SA Health

Contents

1. Policy Statement

The purpose of this Policy Directive is to:

- Provide information and direction on the use of overt and covert surveillance in and associated with SA Health workplaces, including the use of optical surveillance, listening or tracking devices; recording of private conversations; the use of information technology systems; and the communication and storage of data recorded/collected through surveillance.
- Facilitate compliance within SA Health with:
  - the requirements of legislation, including the *Surveillance Devices Act 2016* (SA); and
  - the *Information Privacy Principles (IPPS) Instruction*[1] - Circular No.12 issued by the Department of the Premier and Cabinet

  as these apply to workplace surveillance in and by SA Health.

This Policy Directive applies to all SA Health employees.

The provisions of this Policy Directive must be made applicable to non-employee workers, contractors, students on clinical placements and volunteers in SA Health through the terms and conditions of their contracts, authorisations and licencing agreements to work within SA Health workplaces.

2. Roles and Responsibilities

2.1 The Chief Executive – SA Health
Ensure that this Policy Directive is communicated for implementation across SA Health.

2.2 Chief Executive Officers of Local Health Networks and SA Ambulance Service
Must take reasonably practicable steps and exercise due diligence within their areas of responsibility to ensure:

- The requirements of this Policy Directive are communicated, implemented and monitored.
- Complaints received about a privacy breach in their services are investigated and addressed.

2.3 The Agency Security Adviser
Must take reasonably practicable steps and exercise due diligence to ensure that the requirements of this Policy Directive are communicated, complied with and monitored.

2.4 Directors of Workforce (or equivalent) and Line Managers
Must take reasonably practicable steps and exercise due diligence within their areas of responsibility to ensure the requirements of this Policy Directive are communicated, complied with and monitored.

2.5 Contract Managers, Volunteer Coordinators and Clinical Placement Coordinators
Must make the provisions of this Policy Directive applicable to non-employee workers, contractors, students on clinical placements and volunteers in SA Health through the terms and conditions of their contracts, authorisations and licencing agreements to work, attend or volunteer on SA Health premises.

2.6 Employees and other workers
Must familiarise themselves and comply with the content of this Policy Directive.

[1] Issued on 6 February 2017 or later version.

3. Policy Requirements

3.1 Purpose of surveillance in SA Health workplaces

Surveillance devices are currently used within and by SA Health for a number of legitimate purposes, such as protecting its employees, clients, patients and others from risks in the workplace; and protecting the interests of SA Health as an organisation, e.g. the assets, information, integrity and reputation of SA Health. Examples are the use of camera surveillance, tracking devises, and data surveillance (e.g. monitoring of employees' computer usage).

Surveillance in SA Health must comply with the requirements of the *Surveillance Devices Act 2016* (SD Act) and the *Information Privacy Principles* (IPPs) within the Department of the Premier and Cabinet Circular No. PC012.

3.2 Compliance with the *Surveillance Devices Act 2016*[2]

The Attorney-General's Department website "*What you should know about the Surveillance Devices Act 2016* provides a concise summary of the provisions of the SD Act. Implications for surveillance in SA Health workplaces are outlined below:

3.2.1 Consent from the surveillance subject required

Unless exceptions provided for by the SD Act apply, surveillance in and by SA Health may only occur with the consent of the surveillance subjects. Consent to surveillance may be explicit (verbal or written agreement) or implied (where the persons under surveillance have been made aware of the surveillance). Awareness can be created, for example by:

- Signage or notice at the entrance and throughout the SA Health workplace; and/or
- SA Health polices, including this Policy Directive, applicable to all employees, or
- The terms and conditions of the contracts, authorisations and licencing agreements to work on SA Health sites of the non-employee workers, contractors, students on clinical placements and volunteers.

3.2.2 Installation, use and maintenance of surveillance is restricted

Without authorisation from the appropriate delegate, employees must not install or use surveillance devices within workplaces or property (including vehicles) of SA Health - such as:

- a listening device that overhears, monitors, or audio records *private conversations*[3] without the consent of all the principal parties[4];
- an optical surveillance device on properties (or vehicles) that visually records or observes *private activity* without the consent of all the principal parties;
- a tracking device that determines the geographical location of a person (or their vehicle) without their consent. (This does not prevent a person from using tracking technology to locate and retrieve an object such as their phone or computer); and
- a data surveillance device that accesses, tracks, monitors or records the input/output of information from a person's computer without their consent.

3.2.3 Use of information, material or data derived from surveillance devices is restricted

Unless authorised by the appropriate SA Health delegate, or unless the exceptions provided for by the SD Act apply, employees must not use, communicate, or publish information or material derived from a listening or optical surveillance device in or around a SA Health workplace.

It may be a condition of entry of persons to a SA Health site that no photos or film be taken without consent.

---

[3] A **private conversation or activity** is one where at least one party would not reasonably want or expect to be overheard or observed by anyone aside from those present [s 3 of the SD Act]. Activities which occur in a public place, or in a location or vehicle, which can reasonably be observed from a public place, are not generally considered private for the purposes of the SD Act. However, conversations in a public place could be potentially be considered private for the purposes of the SD Act - depending on whether the parties could reasonably expect the conversation to be overheard by someone else.

[4] Section 4 and 5 of the SD Act.

3.2.4 Compliance with the *Information Privacy Principles*

The IPPs[5] are relevant to surveillance in SA Health as the information collected by such devices is typically private personal information. (See the definition of "*personal information*" in section 6 of this Policy Directive.) The key requirements of Part II of the IPPs are outlined below as these relate to personal information derived from surveillance in or by SA Health.

3.2.5 Surveillance must be lawful and necessary

IPP 1 requires that personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily. Public sector agencies may only collect information through surveillance in their workplaces for legitimate reasons and relevant to its purpose and functions (see 3.2.6 below). Information obtained through surveillance must be acquired in a manner that adheres to legislative requirements and ethical standards where the right to privacy of individuals may be impacted.

3.2.6 Irrelevant personal information must not be collected

IPP 3 requires that personal information collected (e.g. through surveillance) must not be irrelevant to the purpose. Public sector agencies may therefore not collect information (e.g. through surveillance), which is not relevant to a legitimate purposes. For example, surveillance information collected by SA Health must be:

- directly related to the employment relationship between SA Health and the employee;
- directly related to non-employee workers' contracts, authorisations and licencing agreements allowing non-employee workers to work on or attend SA Health premises;
- related to the safety and security of its employees, clients, patients and others; and/or to protecting the assets, information, integrity, reputation or other legitimate interests of SA Health;
- related to the prevention or investigation of alleged/suspected criminal activity or misconduct; or
- other legitimate reason (e.g. authorised or required by or under law).

3.2.7 Excessively personal information must not be collected

IPP 3 further prohibits the collection of excessively personal information. One application of this Principle would be that surveillance equipment must not be used where there exists a reasonable expectation of privacy, such as in patient examining areas, bedrooms, restrooms; change rooms, locker rooms, showers, toilets and bathing facilities. This type of surveillance could further be a contravention of section 26B or 26D of the *Summary Offences Act 1953,* as it could amount to humiliating / degrading filming, or indecent filming.[6]

3.2.8 Notice of surveillance must be given

IPP 2 requires that, before personal information is collected (e.g. surveillance commences), reasonable steps must be taken to advise individuals of this; the reasons for doing this; any authorisation of or legal requirements for this; and the use and disclosure of the information/material/data so collected.

SA Health must therefore notify employees, contractors, visitors and others in its workplaces of any surveillance; e.g. through notices at the entrance of sites where surveillance equipment is used; through SA Health policies on surveillance or by specific notification of new surveillance in particular areas. (Refer to 3.3.2 below for detail on its practical application in SA Health.)

3.2.9 Storage etc. of personal information

IPP 4 requires that public sector agencies must take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused. (More detail on implementation of this Principle is in 3.3.17.)

3.2.10 Access to records/recordings of personal information

IPP 5 requires that, where an agency has in its possession or under its control records of personal information, access to those records may be obtained in accordance with the *Freedom of Information Act 1991*.

---

[5] The IPPs apply to "*public sector agencies*" as defined in clause 3 (1) of the *Public Sector Act 2009,* which includes SA Health. IPP 4 states that: "*The principal officer* (Chief Executive) *of each agency shall ensure that the following Principles are implemented, maintained and observed for and in respect of all personal information for which his or her agency is responsible".* IPP 6 requires that: "*An agency shall not do an act or engage in a practice that is in breach of or is a contravention of the Principles*".

[6] This, however, does not preclude Local Health Networks from facilitating surveillance in the bedrooms or private areas of aged care recipients where this is requested or consented to by the aged care recipients (and/or others legally authorised to act on their behalf) and has been consulted with stakeholders. (Refer to 3.3.18.)

3.2.11 Use of personal information

IPPs 7 and 8 require that personal information (e.g. as obtained through surveillance) must not be used except for the purpose of its collection -. The exceptions are:

- where the subject can reasonably expect the information will be used for the secondary purpose;
- the record subject has expressly or impliedly consented to this use;
- the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;
- the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty; or for the protection of the public revenue; or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;
- the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- the agency reasonably believes that the use relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and
  - the agency reasonably believes that the use is appropriate in the circumstances; and
  - the use complies with any guidelines issued by the Minister for the purposes of this clause.

3.2.12 Disclosure of personal information

IPP 10 limits the disclosure of personal information as follows:

"An agency should not disclose personal information about some other person to a third person for a purpose that is not the purpose of collection (the secondary purpose) unless:

(a) the record-subject would reasonably expect the agency to disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;

(b) the record-subject has expressly or impliedly consented to the disclosure;

(c) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person;

(d) the disclosure is required or authorised by or under law;[7]

(e) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer;

(f) the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the agency reasonably believes that the disclosure relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and

(i) the agency reasonably believes that the disclosure is appropriate in the circumstances; and

(ii) the disclosure complies with any guidelines issued by the Minister for the purposes of this clause."

3.2.13 Unlawful activity, illegal conduct or serious misconduct

For SA Health to rely on IPPs 7, 8 or 10 to use personal information obtained through surveillance for a secondary purpose such as to investigate concerns, a reasonable suspicion of unlawful activity, illegal conduct or serious misconduct must be present before such use. (See also 3.3.3, 3.3.5 and 3.3.12 below.)

[7] Refer to 3.3.14: Disclosures may be required or authorised by an exemption specified within section 93 of the *Health Care Act 2008* or section 106 of the *Mental Health Act 2009*.

3.3 Practical implications in SA Health

3.3.1 Approval of general surveillance in SA Health

Persons in SA Health who may approve the installation, use and management of surveillance, include (as relevant): the Chief Executive, Chief Executive Officers, the Chief Information Officer; those with delegated authority in Audit and Assurance; Workforce/People and Culture; eHealth Systems Security and/or the Agency Security Adviser. Any CCTV application within SA Health should be designed, implemented and operated in full consultation with the Agency Security Adviser.[8] Approval of surveillance in SA Health must be for legitimate reasons (see 3.2.6) and must comply with legislation; the IPPs and this Policy Directive.

3.3.2 Notice of surveillance prior to commencement

Notice of surveillance in the workplace must be given prior to this commencing, unless:

- the surveillance is subject to a specific exemption by the Chief Executive or Chief Executive Officer (as in section 3.3.5 below); or
- the surveillance is by and/or authorised by a person in a law enforcement agency or an inquiry agency as defined in the *Independent Commissioner Against Corruption Act 2012.*

Notice is required as follows:

- Signage must be erected at the entrance to areas under optical surveillance to advise employees and others that they are entering an area under such surveillance. Signage should address language barriers, including the use of symbols.
- Employees must be advised of the provisions of this Policy Directive (e.g. in hard copy or through publication via the Policy Distribution System) and must be able to access this Policy Directive on the SA Health intranet and internet.
- New employees must be advised of their obligations to comply with SA Health policies (including the *Workplace Surveillance Policy Directive*), when commencing work (e.g. during induction).
- Non-employee workers must be made aware of the requirements of this Policy Directive through the terms and conditions of their contracts or agreements authorising them to work on SA Health sites.
- As necessary, employees and other workers should periodically be reminded of (the possibility of) surveillance in SA Health facilities and by authorised employees of SA Health.
- Where new surveillance in a specific area is intended, employees and relevant employee associations have to be provided 14 days' advance notice of:
    - the kind of surveillance intended (e.g. camera, computer, or tracking);
    - the reasons for the surveillance;
    - authorisation of, or legal requirements of the surveillance;
    - when the surveillance will commence;
    - whether the surveillance will be continued or intermittent;
    - whether surveillance will be for a specified limited period or ongoing; and
    - the use and disclosure of the information collected.

3.3.3 Optical surveillance devices must be visible

As a general rule, video cameras (camera housings) must be installed in a clearly visible manner in the location where video surveillance is to take place (i.e. surveillance should not be covert).

3.3.4 Approval of video surveillance

Where management wishes to have new video surveillance equipment installed within or outside a SA Health area, a formal request must be made to and written approval received from the Chief Executive or Chief Executive Officer of the relevant Local Health Network/SA Ambulance Service/Health Service and/or from the Agency Security Adviser. It is recommended that advice from the Agency Security Adviser is sought for such approvals[9].

[8] New surveillance must be consistent with the SA Health Security Standards. The Agency Security Adviser can provide advice on relevant requirements at the time when new surveillance is considered. Advice should also be obtained from the Agency Security Adviser as to the purchase of appropriate surveillance cameras/equipment.

[9] Refer to 3.3.1.

Requests for approval of new video surveillance must address the following:

- the purpose for the proposed surveillance and collection of information;
- who will conduct and oversee the surveillance (and whether there are any related investigations);
- when the surveillance will commence;
- the area(s) that will be covered by the surveillance;
- whether the surveillance will be continuous or intermittent;
- persons/authorities to whom the information obtained from the surveillance will or may be provided; and
- how notice of the proposed surveillance will be given to affected persons.

An employee who contributes to, or attempts to contribute to the installation of camera surveillance (including imitation surveillance equipment or casings) without having obtained the requisite approval, may be liable to disciplinary action.

3.3.5 Approval of covert video surveillance

Covert surveillance must not be used except for the purposes of detecting suspected unlawful / criminal activity in the workplace. It may not be used merely to monitor employees (e.g. whether they are present, performing as required or for any other monitoring purpose).

Where management desires to have covert video surveillance equipment installed within or outside a particular SA Health area, the following matters (in addition to those listed in section 3.3.4) must be addressed in a formal written request to the Chief Executive or Chief Executive Officer:

- the basis of the suspicion that one or more employees are involved in unlawful activity;
- any agency/ies that the suspected conduct has been reported to (e.g. the Office for Public Integrity; the Independent Commission Against Corruption or the SA Police – Anti-Corruption. Branch);
- whether any other managerial or investigative procedures have been undertaken to detect the unlawful / criminal activity and the outcome of these procedures; and
- when the surveillance will conclude.

The apparent seriousness of the suspected unlawful activity will determine whether there are sufficient grounds for covert surveillance.

The Chief Executive or Chief Executive Officer must be satisfied that the covert surveillance of the employee(s) will not unduly intrude on the privacy of any other individual; and should be able to justify their approval of the covert surveillance should the Privacy Committee of South Australia investigate complaints relating to the covert surveillance or regarding alleged violations of individual privacy.

3.3.6 Prohibited locations

Surveillance in any area where there exists a reasonable expectation of privacy such as in patient examining areas, bedrooms, restrooms, change rooms, locker rooms, showers, toilet and bathing facilities, etc.is strictly prohibited.[10] Advice must be obtained from the Agency Security Adviser on the acceptability of surveillance in seclusion rooms.

3.3.7 Recording of private conversations

The installation, use or maintenance of a listening device to overhear, record, monitor or listen to private conversations is prohibited. Unless the exemptions under section 4 and 6 of the SD Act apply, private conversations should not be recorded; and visual surveillance, whether overt or covert, must not contain listening devices or have capability to record conversations. Some of the exceptions that apply are where:

- The parties to the conversation consent to the use of a listening device.
- A listening device is needed to protect the lawful interests of a person.
- The use of the device is in the public interest.
- The use is specifically authorised by legislation (e.g. the *Telecommunications (Interceptions) Act 1979 (*Cth); *Part 2 of the Criminal Investigation (Covert Operations) Act 2009;* or the *Security and Investigation Industry Act 1995*).

[10] This, however, does not preclude Local Health Networks from facilitating surveillance in the bedrooms or private areas of aged care recipients where this is requested or consented to by the aged care recipients (and/or others legally authorised to act on their behalf) and has been consulted with stakeholders. (Refer to 3.3.18)

3.3.8 Surveillance of employee's use of information and communications technology (ICT)

SA Health has a responsibility to protect and monitor the content of information sent through its electronic communications. Such monitoring is undertaken for all SA Health electronic communications activities.

Employees' and other workers' use of information and communications technology (e.g. emails, use of the internet or access to databases) may be monitored for legitimate purposes; e.g. to ascertain that the use of ICT systems, computers, databases and related facilities is appropriate; to investigate suspected or alleged breaches of acceptable use; or as part of an investigation of suspected/alleged misconduct or illegal activity.

Under certain circumstances, the Chief Executive, Chief Executive Officers, the Chief Information Officer of SA Health or the Agency Security Adviser may approve requests for eHealth Systems Security to report on or investigate email and internet activities. This may involve accessing, reviewing and disclosing details of electronic communications use. (Refer also to SA Health's Electronic Communications Policy.)

3.3.9 Monitoring of employee access to SA Health workplaces

The Chief Executive, Chief Executive Officers or those with delegated authority may, for purposes stated under 3.2.6, approve monitoring of individual employee's access to SA Health buildings, sites or areas (e.g. via examining the use of security access cards or by existing CCTV surveillance).

3.3.10 Tracking of SA Health vehicles

The Chief Executive, Chief Executive Officers; Agency Security Adviser or those with delegated authority in Audit and Assurance, and Workforce/People and Culture may approve, for purposes stated under 3.2.6, the use of tracking devices indicating the geographical location of SA Health vehicles. It is recommended that advice from the Agency Security Adviser is sought for such approvals.

3.3.11 Approval of investigative surveillance

When seeking approval to proceed with investigative surveillance, the investigating officer must provide the Chief Executive, Chief Executive Officer or Chief Information Officer a brief synopsis of the following:

- The allegations/complaint being investigated.
- The nature of surveillance required.
- The purpose of the surveillance and how the data obtained will be used.
- How the information obtained will be safeguarded and managed.
- The individuals/authorities that will be involved in the investigation and will have access to the data obtained.
- Duration of the surveillance or indication of when the investigative investigation will be concluded (e.g. reference to date or an event.)

Refer also to 3.3.12.

3.3.12 Surveillance related to worker's compensation claims

Pursuant to the IPPs, public sector agencies, including SA Health, must at all times respect an injured employee's integrity, confidentiality of their personal information and right to privacy. A reasonable suspicion of dishonesty or fraudulent activity must therefore be present before surveillance of an injured worker may commence.[11] This surveillance must therefore only be approved in such circumstances. The Director of Workforce (or equivalent) or Workforce Health and Injury Management Manager may approve this.

3.3.13 Access to data

Access to data/information derived from surveillance is restricted to the Chief Executive, Chief Executive Officers, Agency Security Adviser or those with delegated authority (e.g. in Audit and Assurance; Workforce/People and Culture; eHealth Systems Security, Freedom of Information Officers, etc.).

[11] A reasonable suspicion means there is a rational basis for the suspicion. Whether or not this suspicion is reasonable will depend on the facts which the suspicion is based upon and the plausibility of these facts.

Other than when providing information to a law enforcement or inquiry agency as required, a delegate must not give others access to information/material derived from surveillance, unless the disclosure is:

- for a legitimate purpose related to the employment of staff or other legitimate business activities of SA Health;
- for the purpose of responding to an application under the *Freedom of Information Act 1991;*
- for a purpose that is directly or indirectly related to civil or criminal proceedings (where authorised); or
- of such a nature that they reasonably believe it to be necessary to avert an imminent threat of serious violence or of substantial damage to property.

Any delegate or decision maker with an actual or perceived conflict of interest in specific surveillance data must not access such information and must withdraw from decision-making on the matter.

Surveillance information must not be accessed:

- in ways which are inconsistent with the obligation on decision makers to act impartially;
- to improperly cause harm, detriment or embarrassment to any person or body;
- to improperly influence others in the performance of their duties or functions;
- for voyeuristic purposes;
- for the advantage of any person or body; or
- to justify the acceptance of any immediate or future gift, reward or benefit from any person or body for themselves or for any other person or body.

Any employee acting contrary to these requirements, i.e. inappropriately accessing personal information, may be liable to disciplinary action.

3.3.14 Disclosure of personal information / surveillance data

Persons that fall within the scope of this Policy Directive must not disclose personal information obtained through surveillance in or by SA Health unless:

- authorised by the Chief Executive; or
- in the case of information obtained while working at an incorporated hospital or in the SA Ambulance Service (SAAS), authorised by the Chief Executive Officer of the hospital or SAAS (as relevant);
- unless the disclosure is required or authorised by an exemption specified within section 93 of the *Health Care Act 2008* or section 106 of the *Mental Health Act 2009*; or
- in accordance with the *Freedom of Information Act 1991*.

The unauthorised disclosure of personal information obtained in SA Health is an offence under the *Health Care Act 2008* and the *Mental Health Act 2009*.

The Chief Executive and Chief Executive Officers of the LHNs and SA Ambulance Service may authorise the disclosure of personal information in accordance with the IPP Instruction for a purpose other than that permitted under section 93 of the *Health Care Act 2008* or section 106 of the *Mental Health Act 2009.*

3.3.15 Authorising disclosure of personal information

Section 93 of the *Health Care Act 2008* and section 106 of the *Mental Health Act 2009* outline the circumstances under which personal information obtained in SA Health may be disclosed. These sections take precedence over IPP 10.

The Chief Executive and Chief Executive Officers of the LHNs and the SA Ambulance Service can authorise the disclosure of personal information in accordance with the IPPs for a purpose other than that permitted under section 93 of the *Health Care Act 2008* or section 106 of the *Mental Health Act 2009.*

3.3.16 Access to surveillance recordings

Access to surveillance material in SA Health (including surveillance material) may be obtained in accordance with the *Freedom of Information Act 1991.* (Refer to IPP 5.)

3.3.17 Retention, download and storage of surveillance data

Data derived from surveillance activities must be retained and stored in accordance with the *State Records Act 1997* and the *Disposal Schedules* issued under that Act.

SA Health must take reasonable steps to ensure that personal information from surveillance in its possession or under its control is securely stored and is not misused - consistent with IPP 4.

Where data is required to be physically stored, it must be downloaded/copied onto an appropriate storage device, such as a compact disc, USB flash drive or hard drive and kept in secure storage. Approved persons must ensure that the data is protected against loss, unauthorised access, disclosure, modifications and/or other misuse. Security measures may further include:

- physical measures, e.g. locks and swipe cards for monitoring data storage areas; or
- electronic measures, e.g. passwords for accessing the surveillance equipment; including access, retrieval, copy and encryption of the data.

Where data is downloaded/copied by an approved person, a register must be kept which details:

- the record of the Chief Executive/Chief Executive Officer's approval to commence extraction and retention of this data;
- the date the data was downloaded or copied;
- the camera serial number (if the camera is an SA Health asset) and its location;
- the date the data was captured by the camera;
- a brief description of the incident that has been downloaded/copied;
- the time period covered by the downloaded/copied footage;
- the purpose for which the data was downloaded/copied e.g. evidentiary purposes for suspected criminal activity and/or misconduct in the workplace or in response to an FOI request;
- the recipient of the data;
- the medium onto which the data was downloaded/copied;
- the title of the record and the location where the copied data will be stored[12;] and
- the name and signature of the authorised person who downloaded or copied the data.

Where data is downloaded/copied and provided to Police for evidentiary or investigative purposes, a SAPOL field receipt must be obtained from the requesting Police and recorded in the above register.

3.3.18 Surveillance in aged care

For quality, safety and security reasons, SA Health may install or facilitate reasonable surveillance within and around its aged care workplaces, including in common and public areas; and - after consultation with stakeholders - in private areas with the consent of the care recipients and/or others legally able to act on their behalf. Surveillance in common areas is conditional on clear signage notifying staff, care recipients and visitors of this surveillance.

It is recommended that written consent to surveillance is obtained from surveillance subjects in circumstances where there exists a reasonable expectation of privacy.

To facilitate installation and use of surveillance in aged care bedrooms or private areas, the Office for Ageing Well in the Department for Health and Wellbeing or the LHNs (in consultation with stakeholders) may:

- Develop guidelines/procedures for the installation and use of this surveillance in bedrooms or private areas of aged care recipients (if requested or consented to by aged care recipients and/or by those with the legal authority to act on their behalf).
- Provide a standard consent agreement between LHNs and an aged care recipient (and/or by those with the legal authority to act on their behalf) consistent with the above requirements. [13]

3.3.19 Grievances

Where there is or has been an alleged contravention of the IPPs or breach of individual privacy in SA Health, employees may make a complaint to the Privacy Committee of South Australia. The Privacy Committee is authorised to investigate or refer for investigation complaints concerning violations of individual privacy.

Complaints about the unlawful use of personal information may also be made to an appropriate Executive Officer in SA Health, or may be referred to entities such as the Health and Community Services Complaints Commissioner, Australian Health Practitioner Regulation Agency, or Ombudsman (as the case requires). Regardless of how a complaint is received, SA Health will be

[12] Where possible - e.g. this detail may not be precise if the data is provided to a third party (i.e. SAPOL, ICAC or FOI recipient.

[13] It is recommended that the provisions of the guideline/procedures and standard consent agreements be reviewed 6 months after the introduction of video surveillance in SA Health managed residential facilities to ensure the consent provisions and protections are appropriate.

required to justify that its collection, use or disclosure of personal information was within the legislative, statutory and policy requirements applicable to SA Health and the *Information Privacy Principles* Instruction.

Employees employed under Part 7 of the *Public Sector Act 2009*, who are aggrieved by an employment decision (as defined under that Act) that directly affects them and pertains to surveillance or access and disclosure of such data, may also apply for review of the decision in accordance with sections 59 to 62 of that Act and sections 26 to 28 of the *Public Sector Regulations 2010*.

Employees employed under the *Health Care Act 2008*, who have a concern about a decision regarding surveillance or access and disclosure of such data, may request a review of this decision in writing to the Chief Executive Officer or Chief Executive within seven days of being notified of the decision. The Chief Executive Officer or Chief Executive must review the decision and advise the employee of the outcome in writing. If the matter is not resolved at the local level, the employee may lodge an application to have their grievance reviewed by the Grievance and Reclassification Appeal Panel within the Department for Health and Wellbeing. [Refer to Part 3 Grievances and Disputes in the *SA Health (Health Care Act) Human Resources Manual*.]

4. Implementation & Monitoring

Compliance with this Policy Directive must be audited and relevant authorities notified as appropriate. As directed by the Chief Executive, the Agency Security Adviser is responsible for monitoring the appropriateness of surveillance by and within SA Health.

The Chief Executive and Chief Executive Officers are required to furnish to the Privacy Committee of South Australia such information as the Committee may require; and must comply with any requirements determined by the Committee concerning the furnishings of that information including:

- the action taken to ensure that this Policy Directive is implemented, maintained and observed in the agency for which he or she is responsible;
- the name and designation of each officer with authority to ensure that this Policy Directive is so implemented, maintained and observed; and
- the result of any investigation and report as requested by the Committee in relation to the agency for which he or she is responsible and, where applicable, any remedial action taken or proposed to be taken in consequence.

5. National Safety and Quality Health Service Standards

N/A.

6. Definitions

In context of this document:

aged care *means* aged care facilities managed by SA Health; including residential aged care facilities (Commonwealth funded) and accommodation options for older people (state funded).

collects *means* gathering, recording, or acquiring personal information from any source and by any means.

consent *means* that an individual has authorised their personal information to be used for a defined purpose or handled in a particular manner. Consent may be *expressed* (i.e. given orally or in writing) or *implied* (i.e. reasonably inferred from the conduct of the individual).

disclosure means the communication or transfer of information, through giving a copy of the information to another organisation or individual, allowing another organisation or individual to have access to the information or giving out summaries, or giving the information in any other way. This is separate to use, although the privacy requirements apply to both the disclosure and use of personal information.

holds as defined under the *Freedom of Information Act 1991*, an agency will be taken to hold a document if the agency has an immediate right of access to the document.

lawful means an act that is authorised, sanctioned, or not forbidden by the substance of law.

personal information means information or an opinion, whether true or not, relating to a person, or the affairs of a person, whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

primary purpose *means* the dominant purpose for which information is collected. Most often in the health system the primary purpose will be to provide care, or an episode of care.

privacy *means* an individual's right to have their personal information protected from unauthorised access or disclosure. In the context of this Policy Directive the term privacy also covers the *principle of confidentiality* whereby any personal information held by SA Health is not disclosed unless authorised.

reasonable the term reasonable is referenced throughout this Policy Directive e.g. reasonable steps, reasonably necessary. It should be taken to *mean* how an individual, who is properly informed, would be expected to act in the circumstances.

reasonable suspicion means there is a rational basis for the suspicion, i.e. the suspicion is based on facts and those facts are plausible.

secondary purpose *means* the use or disclosure of personal information for a purpose other than the purpose for which it was collected.

7. Associated Policy Directives / Policy Guidelines and Resources

This Policy Directive should be read with:

- *Australian Standard AS4806.1 –2006 Closed Circuit Television – Management and Operation*
- *Code of Ethics for the South Australian Public Sector*
- *Criminal Law Consolidation Act 1953 (SA)*
- *Department of the Premier and Cabinet Circular Information Privacy Principles (IPPS) Instruction*
- *Directions and Guidelines of the Independent Commissioner Against Corruption*
- *Freedom of Information Act 1991 (SA)*
- *Health Care Act 2008 (SA)*
- *Independent Commissioner Against Corruption Act 2012 (SA)*
- *Mental Health Act 2009*
- *Public Sector Act 2009 (SA)*
- *SA Health (Health Care Act) Human Resources Manual.*
- *SA Health Privacy Policy*
- *State Records Act 1997 (SA) (*and the *Disposal Schedules* issued under the Act)
- *Surveillance Devices Act 2016 (SA) and Surveillance Devices Regulations 2017*

Related SA Health Policies are available on the SA Health Policy Distribution System, e.g.:
Privacy Policy Directive; Protective Security Policy; Electronic Communications Policy; Information Communication Technology Security Policy; Acceptable Use Policy ;Fraud and Corruption Control Policy Directive; and the South Australian Public Sector Fraud and Corruption Control Policy.

8. Document Ownership & History

Document developed by: HR & Workforce Services, Corporate & System Support Services.
File / Objective No.: 2018- 11735
Next review due: 22/07/2024 (5 years after approval)
Policy history: Is this a new Policy Directive (V1)? No
Does this Policy Directive amend an existing Policy Directive version? Yes.
Does this Policy Directive replace another Policy Directive with a different title? Yes. Acceptable Surveillance Policy Directive V2.

ISBN No: **978-1-76083-158-5**

Approval Date	Version	Who approved Version	Reason for Change
22/07/2019	V3.0	SA Health Policy Committee	Amended in line with legislation and to enable correct practice.
25/11//2016	V2.0	Portfolio Executive	Amended after consultation with stakeholders.
16/01/2016	V1.0	Portfolio Executive	Original approved version.