ACSA Working Paper

ACSA
Aged & Community Services Australia

SURVEILLANCE TECHNOLOGIES IN RESIDENTIAL AGED CARE

ACSA has developed this paper in response to public discourse and subsequent member requests for a guidance document containing key issues to consider in relation to surveillance devices in residential aged care facilities. The paper provides guidance across a range of topics including governance, staffing, working with families, legislation and regulation.

~~~

ACSA endorses the ethical and lawful use of surveillance in residential aged care where reasonably necessary to protect the safety of residents, and where it does not unreasonably impinge, or render unbalanced, their rights under the Charter of Aged Care Rights, or undermine the rights of staff. It is important there are clear policies, procedures and governance processes in place regarding surveillance, taking into account jurisdictional considerations.

Aged Care providers want to ensure the best quality of care for their residents. Fundamental to this is honouring their rights as human beings and ensuring they are safe.

Aged care providers have zero tolerance for criminal abuse, assault or negligence. Poor or inattentive care has no place in our sector.

Responding to the risk of elder abuse in residential aged care may involve a range of strategies including the use of surveillance to ensure the safety of residents. The use of surveillance involves balancing safety with other rights including privacy and dignity.

There is a community conversation about the use of surveillance technologies in aged care as a means of identifying and acting where abuse is found to have occurred. Many aged care providers already use such technologies in common areas. In addition, the Federal Government announced a trial of using CCTV in residential care in South Australia as part of its election campaign. A number of
~~~

aged care facilities managed by SA Health will have CCTV cameras installed as part of this year-long 500,000 trial. SA Premier Steven Marshall said his government would deliver the pilot in partnership with audio-visual monitoring company Care Protect[1].

The development of a cooperative approach between provider, older person (or their decision maker) and families is paramount to any use of monitoring and surveillance within aged care facilities.

The use of such technologies is not a substitute for training, recruitment and management of staff and astute governance to ensure residents' privacy and right to safety in residential care.

Surveillance legislation (including workplace surveillance) in Australia is complex and varies state by state. All states have legislation governing audio surveillance, while regulation of optical surveillance is more erratic.

Surveillance has an impact on aged care staff. Some states have specific workplace surveillance legislation. Depending on jurisdiction, consent may be required from one party, all parties, and/or the owner/occupier of the premises on which the surveillance device is installed. Whether surveillance is lawful may depend on who installed it – i.e. the resident, their family, or the aged care provider.

The use of surveillance may constitute a criminal offence under state/territory surveillance laws, and attract penalties under the Commonwealth Privacy Act 1988.

This paper provides guidance for the use of surveillance devices in residential aged care settings to assist them in developing their own policies and protocols, however it is not meant to be prescriptive, nor is it a substitute for legal advice. Given the law around surveillance varies between states and territories, it is recommended that legal advice is obtained in relation to any proposed policy for individual providers.

GUIDING PRINCIPLES

Clear principles[2] should be developed and set the organisational tone and communicate your intentions with the use of surveillance. They provide an overarching statement for residents, families, staff and the community about your views and their context. They should accompany a statement/policy about elder abuse. When developing principles to guide your organisation, you should familiarise yourself with:

- The legislation that applies in your state/territory (see 'Legislation' section below) to ensure you are familiar with the lawful circumstances in which surveillance may be used; and
- The Charter of Aged Care Rights (see '*Charter of Aged Care Rights*' section below).

ACSA's 2016 Position Paper on Elder Abuse can be found here.

Privacy

Privacy is a fundamental right for all Australians enshrined in the UN Declaration of Human Rights, to which Australia is a signatory[3].

It is also a right under the Charter of Aged Care Rights. The Aged Care Quality Standards (the Standards) also recognise an individual's right to privacy and to be treated with respect[4].

Surveillance should only be undertaken with consideration of how the privacy of everyone impacted is respected and protected.

The Privacy Act applies to aged care providers across Australia and any surveillance policy developed must be in line with the Act and your privacy policies. You should also consider your obligations around the handling of personal information under the Privacy Act, and the significant penalties associated with any privacy breaches.

[1] Australian-first CCTV trial for aged care facilities as elder abuse continues to be captured – ABC News (Australian Broadcasting Corporation), Briggs C. and Slessor C, Updated 11 April 2019

[2] A reference when considering the development of guiding principles see (Egan 2015; Fisk & Flórez-Revuelta 2016), https://www.academia.edu/29390240/The_ethics_of_using_cameras_in_care_homes

[3] CCTV in Residential Aged Care Bedrooms, Fuss M. Senior Associate O'Loughlins Lawyers, December 2018.

[4] Aged Care Quality Standards, Standard 1 Consumer dignity and choice, 1.2 (C), Aged Care Quality and Safety Commission, Australian Government

Key resident and staff issues to be considered include:

- *Residents* – balancing the potential to protect residents from mistreatment or abuse versus the impact of such devices on privacy;

  Where residents have the capacity to consent (or withhold their consent) then their right to exercise choice and control must be respected by all concerned. Where consent is not obtained from the resident or their substitute decision maker then CCTV surveillance should not be used (unless required by law, warrant or other authorisation);

  The right to privacy is paramount when considering the introduction of surveillance in a resident's room where intimate care and personal hygiene activities are undertaken.

  Additionally, a resident's privacy is to be considered (and their consent gained – see '*Consent*' section), when installing surveillance devices in areas where they may reasonably expect their activities are private, for example any activity in the privacy of their room or in semi-private areas.

  Staff – also have rights and their privacy may be compromised with the introduction and use of such devices. To this end:

  - Clear signage regarding surveillance should be in place for communal and work areas; and
  - Surveillance should not be installed in work areas where staff should reasonably expect privacy, including workplace toilets, washrooms; change rooms or lactation rooms. The use of surveillance devices in these areas may constitute an offence under state/territory legislation around surveillance, including workplace surveillance. Providers need to be cognisant of the relevant legislation in their state / territory in addition to the Privacy Act and seek legal advice if considering installing surveillance in any work area.

Consent

Consent is a key issue to be addressed prior to the introduction of surveillance technology. Each state/territory has slightly different surveillance consent requirements and under the Commonwealth Privacy Act 1988 ('Privacy Act'), which applies nationally, there must be consent to collection of any personal information. The Australian Law Reform Commission (ACLRC) Report[5] on Elder Abuse describes 'promoting autonomy and agency of older people' as an essential framing principle. The principle of autonomy underpins consent, which in turn impacts on the lawfulness of surveillance. Policies and procedures addressing consent should include the following components:

- The procedure for obtaining consent and how often this consent will be reviewed;
- The procedure for when consent is withdrawn;
- The procedure when consent is limited to surveillance at certain times only;
- The processes in place to manage the rights of residents, representatives, visitors and staff (including volunteers) who do not consent;
- The circumstances in which surveillance footage may need to be disclosed as a matter of law;
- The inclusion of surveillance clauses in resident agreements; and
- Signage requirements notifying all parties of the presence and location of surveillance cameras.

Consent to record images should be gained from:

- *Residents* –in private areas (for example resident rooms) and semi-private areas (such as small lounges or sitting areas) where the resident would have a reasonable expectation of privacy. Consent may not be required in communal settings (for example dining rooms, activities areas etc.) provided surveillance is not covert and specific state legislative requirements are considered. Providers should understand whose consent is required in their jurisdiction, and when (and hence the legislative distinction between private and public activities).

[5] Elder Abuse – A National Legal Response, Final Report, Australian Law Reform Commission, Australian Government, May 2017, p69

Consent should be gained from the resident/s impacted, or where this is not possible (due to cognitive decline or other reasons) from their authorised substitute decision maker. Providers should check the legal authority required in their state/territory for the substitute decision maker to give consent to surveillance. For example, a power of attorney may not be sufficient authority and a guardianship with specific powers to consent to surveillance on behalf of a resident may be required.

ACSA supports the view in the ALRC report on Elder Abuse that 'appointed decision makers should support and represent the will, preferences and rights of the principal[6], that is the substitute decision maker should base their consent to surveillance of the resident on what they believe the resident would wish or state were they in a position to do so.

- *Families* – families should be informed of the intention to use surveillance devices, including explaining the rationale, the types of devices used and their locations. If family members are surveilled in a resident's room, then in some state/territories their consent may also be required.
- *Staff* – best practice would include proactive conversations and communication with staff in relation to the installation of monitoring devices, including at the time new staff are engaged. There are obligations to notify or consult with staff in some states/territories, and specific staff consent to surveillance may be required in respect of surveillance in a resident's room, even if the resident consents (depending on the jurisdiction).

Failure to gain explicit or implied consent from the parties concerned, prior to the introduction of surveillance, may constitute an offence under surveillance devices legislation. Providers should consider if consent is required from anyone who will be under surveillance.

Organisational governance of surveillance practices

Standard 8 of the Aged Care Quality Standards requires, among other things, that consumers are 'engaged in the development, delivery and evaluation of care and services and are supported in that engagement'. Providers, when considering the introduction of workplace surveillance should understand and address key principles including (but not limited to):

- Allocating responsibility for the surveillance program to a person within the organisation (this could be for example the Privacy Officer or similar);
- Developing policies and procedures that address privacy principles and surveillance activities (could include the development of privacy checklists, guidelines[7] and/or manuals), including issues such as:
    - Access to surveillance recordings (by resident, family, other parties etc.);
    - Ownership of surveillance data;
    - Use, storage and destruction of surveillance recordings;
    - Disclosure requirements under law;
    - Review of surveillance footage (periodic or otherwise), and
    - Consent (as discussed).
- Monitoring and review of surveillance activities through the organisation's governance and risk management processes;
- Ensuring complaints processes and procedures include complaints related to the surveillance program;
- Developing protocols and processes to respond to resident/family requests to install surveillance devices;
- Developing protocols to respond to data breaches or other suspected breach of privacy; and
- Considering how to respond to any unlawful or covert surveillance device/s discovered, including protocols for staff to follow should they discover an unlawful surveillance device.

[6] Ibid, p164

[7] Guidelines developed by providers may include articulating the 'legal authority' that the organisation requires for a substitute decision maker to be giving consent that impacts on the resident's right to privacy

Staffing matters

The use of surveillance is not a substitute for comprehensive training and education and appropriate managerial oversight of day to day operations[8].

Best practice would indicate staff are fully informed of the use surveillance devices in the workplace, including explaining the rationale and benefits of the use of surveillance devices, the types of surveillance devices used and their location (in particular, whether they might be in residents' private rooms in addition to public/communal areas. Consent requirements in relation to staff need to consider relevant state/territory surveillance and workplace legislation.

The use of surveillance devices should be discussed with new staff at the time of their engagement.

As there is likely to be staff anxiety and concern in relation to surveillance in their workplace the positive benefits of surveillance should be explained to staff, positive benefits may include:

- reducing the risk of resident abuse;
- assisting in monitoring risk;
- responding to workplace health and safety incidents; and
- upholding employees' rights to be safe at work.

Staff rights to privacy are addressed in the *Privacy* section above.

Working with families who install a camera

Experience suggests families install covert surveillance where they have concerns about care delivery. Where a provider identifies that family has installed covert surveillance in a resident's room:

- Constructively engage with the family to understand their concerns;
- Where warranted, undertake an investigation of the family's concerns;
- If care deficits are identified, an open disclosure approach should be used.

Family members of residents are bound by legislation in relation to installation of surveillance devices. If they have installed surveillance devices without appropriate consent, they may be committing an offence.

If the provider becomes aware of a covert surveillance device then consideration needs to be given to how to respond. The following approach could be considered:

- Determining whether to leave the device in place, turn it off or remove it. Providers should have protocols in place ready to enact should covert surveillance be detected (an organisation's default position may be for example to remove the device pending confirmation of the legal authority for its installation);
- Informing staff, as soon as practical of the location of the surveillance device;
- Determining whether the resident is aware of the presence of the camera;
- Determining consent:
    - If the resident has capacity, and has consented to the camera being installed, a protocol could be in place to manage subsequent actions, including informing staff; and
    - If the resident does not have capacity, another protocol could be in place addressing subsequent actions to take to determine if there is legal authority from the substitute decision maker;
- Contacting the family to discuss the situation, determining their rationale for installing the device. Such a conversation may provide a positive opportunity to work with the family to address concerns; and
- If the provider has a legitimate concern that appropriate consent has not been obtained then consideration may be given to contacting relevant authorities such as the Office of the Public

[8] Rozenbergs K (2016) CCTV: When policing a problem creates a problem, Aged Care Insite at http://www.agedcareinsite.com.au/2016/06/when-policing-a-problem-creates-a-problem/

Advocate, office of the Australian Information Commissioner[9] or the Police if the situation is deemed to warrant such an approach.

Responding to family requests to install a camera

If families request to install a Surveillance device in the residents' rooms there are a range of issues that are relevant, including.

- Assessing the legal authority of the family member requesting the installation of the surveillance; providers are to have a clear understanding of the legal authority required in their state/territory;
- Understanding and complying with the relevant surveillance and privacy legislation;
- Understanding the family's motivation for the request to install a surveillance device such as CCTV. This may provide a positive opportunity to address family concerns;
- Addressing privacy related matters for the all parties impacted; and
- Addressing consent related matters for all parties impacted by the proposed installation of surveillance (including other family members and visitors).
- Informing staff if a surveillance device is to be installed

Ownership, use, access, storage, disposal of the recorded image and cost should be discussed.

Costs

The costs associated with the installation and monitoring of CCTV footage, as well as data storage costs may be large.

As a guide, universal monitoring by an external service (as proposed in the Commonwealth funded trial in South Australia) and potential subsequent costs is currently listed at $20 per resident per week. For a 100-bed facility this could equate to $104,000 per annum.

Providers need to understand the cost structures involved in contracting external monitoring services, for example whether cost is based on fixed bed numbers or on occupied beds.

Consideration will need to be given to how the costs are covered.

LEGISLATION / REGULATION

Charter of rights

The Charter of Aged Care Rights (the Charter), which came into effect on the 1 July 2019 provides rights to all consumers of Australian Government funded aged care services. The Charter focusses on 14 high-level consumer rights[10] and is given legal status under the Aged Care Act 1997. Providers, when developing their approach to the use of CCTV, should consider a number of the key statements contained within the Charter and how these might impact, and may be addressed, including (but not limited to):

- Number 4: the right to live without abuse and neglect; and
- Number 13: the right to personal privacy and to have my personal information protected.

These rights contained within the Charter must inform a provider's approach in relation to the introduction of CCTV surveillance, ensuring principles such as dignity of risk, privacy and consent are protected.

A consistent principle across the various legislative frameworks is that private activities and conversations cannot be recorded without the consent of at least one party involved.

Providers are to be familiar with relevant legislation in their state / territory and seek independent legal advice as necessary. It is beyond the scope of this position paper to list all relevant legislation

[9] https://www.oaic.gov.au/
[10] https://agedcare.health.gov.au/quality/single-charter-of-aged-care-rights

for all states and territories. Broadly it is important that providers identify key state / territory legislation relevant to:

- *Surveillance devices, including listening devices*[11] *and workplace surveillance laws*; and
- *Privacy (including the Privacy Act and state-based privacy legislation)*, and
- *Criminal laws under which the use of surveillance may be captured*.

Separately, providers should consider relevant privacy requirements under the:

- Aged Care Act 1997;
- Privacy requirements under the Aged Care Quality Standards[12] (Standard One); and
- The Charter of Aged Care Rights.

Aged care quality standards

Providers should consider the Aged Care Standards including (but not limited to):

- Standard One[13] – Dignity and choice: This standard requires:
    - Each consumer is treated with dignity and respect – Requirement 3(a);
    - Each consumer is supported to exercise choice and independence, including to make decisions about their own care and the way care and services are delivered – Requirement 3 (c) (i);
    - Each consumer is to be able to exercise choice around the formation of intimate relationships – Requirement 3 (c) (iv);
    - Each consumer's privacy is respected, and personal information kept confidential – Requirement 3 (f); and
- Standard Eight – Organisational governance: This standard requires:
    - The organisation must demonstrate that consumers are engaged in the development, delivery and evaluation of care and services and are supported in that engagement – Requirement 3 (a)

Providers will need to balance and address these requirements, including involving consumers in decision making, respecting their views and listening to their preferences.

Could the surveillance data constitute health information?

In some circumstances the nature of surveillance data means it constitutes health information, and hence a health record under state or territory legislation. Specific legal advice should be sought in this regard.

Providers should be aware of any health record legislation in their jurisdiction that may apply to surveillance data and the legal considerations around its collection, use/disclosure, storage/retention, and access. For example, in NSW health information collected must be 'relevant' to the purpose for which it is collected, 'not excessive' and must 'not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates[14]'.

Cross-border considerations

If surveillance data is collected via the use of software, providers will need to consider where the data is being stored. There are restrictions on transmitting data overseas under the Privacy Act. Further, if data is stored outside the relevant state, additional consent may be required.

Legal advice should be obtained if data is to be transmitted/stored outside the jurisdiction in which it was collected.

[11] In Tasmania, regulation of visual recording is regulated by s13A of the Police Offences Act 1935, while audio recording falls under the Listening Devices Act 1991
[12] This Standards reference refers to the Aged Care Standards that are coming into force on the 1 July 2019.
[13] These Standards references refer to the Aged Care Standards that are coming into force on the 1 July 2019.
[14] Health Privacy Principle2, Schedule 2, Health Records and Information Privacy Act 2002).

RESOURCES

The ethics of using cameras in care homes, see here. Fisk M. et al, Nursing Times 2016

Are you being watched? The risks of "nanny cams" in residential aged care, see here. Russell Kennedy Lawyers, March 2018

CCTV in residential aged care bedrooms, see here. OLOUGHLINS Lawyers, 2018

REVIEW

ACSA has developed this working paper in response to public discourse and subsequent member requests for a guiding document. Following distribution and allowing for a reasonable time for members to use it[15], we will seek member feedback through our relevant national and state committees.

We are currently exploring having a supporting product available in our Quality Portal.

28 October, Addendum – Overview of Commonwealth and state/territory legislation in Australia

Commonwealth legislation

- *The Privacy Act 1988 (Cth):*

The *Privacy Act* applies to all Australian private health sector service providers, aged care and disability service providers. The *Privacy Act* regulates the collection, use and disclosure of "personal information," including photos which would make a person reasonably identifiable. The *Privacy Act* stipulates that personal information may be collected so long as people are notified their information is being collected and the purpose of the information is reasonably necessary for, or directly related to, one or more of the organisation's activities.

The *Privacy Act* does not cover the use of security cameras operated by individuals acting in a private capacity, however state/territory laws may apply.

Under the *Privacy Act,* personal information is 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 if it is recorded in a material form or not.

- *Australian Privacy Principles* (set out in the *Privacy Act 1988* (Cth)):

The Australian Privacy Principles apply to organisations who have a turnover of over $3 million and/or organisations who collect personal or sensitive information.

Sensitive information includes information about an individual's race, political opinions, membership of political associations, religious beliefs, memberships of professional or trade associations, membership of trade union, sexual orientation or criminal record. It also includes health, genetic or biometric information about an individual.

Principle 5 of the *Australian Privacy Principles* deals with the notification of the collection of personal information. People whose personal information has been collected should be notified before it is collected. If this is not possible, they should be notified as soon as practicable after it has been collected.

- *Charter of Aged Care Rights* (set out in the *User Rights Principles 2014* (Cth))

[15] This paper to be reviewed June 2020.

Organisations should note the right of clients to be treated with dignity and respect, and their right to personal privacy and to have their personal information protected.

States & territories

Summary of states & territories:

Workplace surveillance

NSW, Victoria and the ACT are the only states that have workplace surveillance laws which regulate the surveillance of employees. In all three states it is an offence to conduct surveillance in areas where employees can expect a reasonable degree of privacy, including bathrooms, changing rooms, lactation rooms and shower facilities. In NSW and ACT, the workplace surveillance legislation applies to the use of optical, computer and tracking surveillance devices, but not listening devices, and employees must be notified at least 14 days prior to surveillance being introduced. In Victoria, listening devices are included under workplace surveillance regulations.

Residents

In addition to the workplace surveillance laws mentioned above, some states have surveillance devices legislation regulating the surveillance of and by any persons, not just employees. Surveillance devices laws in NSW, Victoria, Northern Territory and South Australia and Western Australia regulate the use of optical, listening and tracking devices. In Queensland, Tasmania and the ACT, surveillance devices legislation only regulates the use of listening devices. In all states, the relevant legislation regulates the use of these devices in situations where not all parties being monitored have consented to the use of surveillance. There are some exceptions which differ state to state on when surveillance can be conducted without the consent of all parties.

New South Wales

Relevant legislation: *Workplace Surveillance Act 2005* (NSW), *Surveillance Devices Act 2007* (NSW), *Health Records and Information Privacy Act 2002* (NSW)

- *Workplace Surveillance Act 2005* (NSW)

The *Workplace Surveillance Act 2005* applies to optical surveillance, computer surveillance and tracking surveillance of employees in a workplace. Surveillance devices in the workplace can only be used if sufficient notice (at least 14 days) has been given to employees and must not be used in change rooms, toilets, shower facilities or areas where workers can expect a reasonable degree of privacy, or outside the workplace.[16] Covert surveillance must not be undertaken unless a covert surveillance authority has been obtained.[17]

In residential aged care facilities, providers must ensure employees are notified at least 14 days before surveillance measures are introduced and surveillance must not be used in areas where employees can expect a reasonable degree of privacy or outside of the workplace.

- *Surveillance Devices Act 2007* (NSW)

Under the *Surveillance Devices Act 2007* a person must not knowingly install, use or maintain a listening device or optical advice to record, monitor or listen to a private conversation to which the person is not a party, or record an activity which involved the entry onto premises without the expressed or implied consent of the owner/occupier of those premises.[18] A device is still considered a listening device even if it is also capable of recording or transmitting a visual image.

Certain exceptions apply: listening devices may be used if all principal parties to the conversation consent to the listening device being used and the recording is reasonably necessary for the

16 Workplace Surveillance Act 2005 (NSW) ss 10(2), 15, 16.
17 Workplace Surveillance Act 2005 (NSW) ss 10(2), 20
18 Surveillance Devices Act 2007 (NSW) ss 7(1), 8(1).

protection of the lawful interests of that principal party.[19] Listening and optical surveillance devices may be used if a warrant or emergency authorisation is obtained.

- *Health Records and Information Privacy Act 2002* (NSW)

The *Health Records and Information Privacy Act 2002* applies to every organisation that is a health service provider or that collects, holds or uses health information. The *Health Privacy Principles* stipulate that organisations must not collect health information unless the information is obtained for a lawful purpose that is directly related to the function or activity of the organisation and is reasonably necessary for that purpose.[20] The information obtained must not be excessive or intrusive.[21]

Australian Capital Territory

Relevant legislation: *Workplace Privacy Act 2011* (ACT), *Listening Devices Act 1992* (ACT), *Crimes Act 1900* (ACT), *Health Records (Privacy and Access) Act 1997* (ACT)

- *Workplace Privacy Act 2011* (ACT)

The *Workplace Privacy Act 2011* applies to optical devices, tracking devices and data surveillance devices, but not listening devices. The Act requires an employer to provide notice to employees if one of these surveillance devices is used in the workplace, and to consult with employees in good faith before the surveillance is introduced.[22] Notice must be given at least 14 days before surveillance starts, or if the worker agrees to a period of less than 14 days.[23] Employees must be notified of the type of surveillance, when it will commence, whether it will be intermittent or continuous and whether it will be for a specific time or ongoing. All surveillance must also be clearly visible to employees with signs indicating that surveillance is taking place.[24] The *Act* prohibits the surveillance of employees in places such as toilets, change rooms, nursing rooms, first-aid rooms, prayer rooms, and surveillance of employees outside the workplace. The *Act* allows for covert surveillance only if the relevant authority from the court has been received.

In residential aged care facilities workers should be given 14 days notice before surveillance devices are introduced. Employees should be consulted when introducing workplace surveillance policies.

- *Listening Devices Act 1992* (ACT)

The *Listening Devices Act 1992* regulates the use of listening devices for the purpose of listening to or recording a private conversation, and for related purposes. Note that it does not regulate the use of other surveillance devices such as optical surveillance, tracking or data surveillance.

It is an offence under the *Act* for a person to use a listening device with the intention of listening to or recording a private conversation, except in cases where all principal parties have consented.[25] An exception applies if consent has been granted and is considered to be necessary for the principal party's lawful interests.[26]

- *Crimes Act 1900* (ACT)

Capturing visual data of a person where the person would reasonably expect privacy may also constitute an offence under Section 61B of the *Crimes Act 1900* (ACT).[27]

- *Health Records (Privacy and Access) Act 1997* (ACT)

19 Surveillance Devices Act 2007 (NSW) s 7(3).
20 Health Records and Information Privacy Act 2002 (NSW) s 1(1).
21 Health Records and Information Privacy Act 2002 (NSW) s 2.
22 Workplace Privacy Act 2011 (ACT) s 13.
23 Workplace Privacy Act 2011 (ACT) s 3.
24 Workplace Privacy Act 2011 (ACT) s 15.
25 Listening Devices Act 1992 (ACT) s 4(1).
26 Listening Devices Act 1992 (ACT) s 4(3).
27 Crimes Act 1900 (ACT) s 61B.

The *Health Records (Privacy and Access) Act 1997* seeks to provide for the privacy and integrity of, and access to, personal information for health-related purposes. The definition of health service under the *Act* includes aged care services that involve the making or keeping of personal health information.[28]

Victoria

Relevant legislation: the *Charter of Human Rights and Responsibilities Act 2006* (Vic), the *Health Records Act 2001* (Vic) (including the Health Privacy Principles) and the *Surveillance Devices Act 1999* (Vic)

Workplace surveillance

- *Surveillance Devices Act 1999* (Vic)

Under the *Surveillance Devices Act,* it an offence to use an optical device or listening device to carry out surveillance of workers' conversations or activities in workplace toilets, washrooms, change rooms or lactation rooms.[29]

There are limited exceptions: surveillance is permitted in accordance with a warrant or emergency authorisation, in accordance with a law of the Commonwealth, or if required by a condition of a liquor licence granted under *the Liquor Control Reform Act 1998* (Vic).[30]

Residents' rights

- *Charter of Human Rights and Responsibilities Act 2006* (Vic)

Section 13 of the *Charter of Human Rights and Responsibilities Act* provides that a person has the right not to have his or her privacy unlawfully or arbitrarily interfered with by public authorities.

- *Health Records Act 2001* (Vic), *Privacy and Data Protection Act 2014* (Vic)

The *Health Records Act 2001* and the *Privacy and Data Protection Act 2014* covers the handling of health information and personal information held by health service providers in the state public sector[31] and the private health sector.[32] Due to the nature of audio visual footage that surveillance technologies are likely to record in the residential care setting, providers should assume that health information and personal information is likely to be collected. As such, footage captured must be handled in accordance with the requirements of these Acts, including the requirement that health information must only be collected if it is reasonably necessary and, subject to certain exceptions, must only be used and disclosed for the primary purpose for which it was collected. Health Privacy Principle 1 in Schedule 1 to the *Health Records Act 2001* sets out circumstances in which health information may be lawfully collected.

- *Surveillance Devices Act 1999* (Vic)

Under the *Surveillance Devices Act 1999*, it is an offence for a person to knowingly install, use or maintain optical surveillance devices to record or observe a private activity **without the express or implied consent of each party to the activity**.[33] Under the *Act*, a 'private activity' is defined as an activity during which the parties desire it to be observed only by themselves.[34] The Act also applies to the use of listening devices and tracking devices.

28 Health Records (Privacy and Access) Act 1997 (ACT) sch 2 (definition of 'health service').
29 Surveillance Devices Act 1999 (Vic) s 9B.
30 Surveillance Devices (Workplace Privacy) Act 2006 (Vic) s 3.
31 Health Records Act 2001 (Vic) s 10.
32 Health Records Act 2001 (Vic) s 11.
33 Surveillance Devices Act 1999 (Vic) s 7(1).
34 Surveillance Devices Act 1999 (Vic) s 3(1).

Northern Territory

Relevant legislation: *Surveillance Devices Act 2007* (NT), *Information Act 2002* (NT)

- *Surveillance Devices Act 2007* (NT)

The *Surveillance Devices Act 2007* regulates the installation, use, maintenance and retrieval of surveillance devices. The *Act* also restricts the use, communication and public information obtained through surveillance devices. The *Act* prohibits a person from installing a surveillance listening device or optical device to monitor or record a private conversation the person is not a party to and if the person knows the device has been installed without the consent of the other party.[35]

Listening devices and optical devices can be used in limited circumstances: where there is a police warrant, where law enforcement has authority or where an activity or conversation is not private. They can also be used in cases of emergency, where there were reasonable grounds for believing the circumstances were so serious that the device was used in the public interest. If the person seeks to rely on this emergency use, they must within two business days of starting surveillance, provide a written report to a Judge of the Northern Territory Supreme Court.[36]

- *Information Act 2002* (NT)

The *Information Act 2002* provides for public access to information held by the public sector and provides for the correction of personal information held by the public sector. Personal information is government information that discloses a person's identity or from which a person's identity is reasonably ascertainable.

Queensland

Relevant legislation: *Invasion of Privacy Act 1971* (Qld), *Information Privacy Act 2009* (Qld), *Criminal Code 1899* (Qld)

- *Invasion of Privacy Act 1971* (Qld)

The *Invasion of Privacy Act 1971* (Qld) regulates the use of listening devices, however it does not address the regulation of other surveillance devices such as optical surveillance, tracking and data surveillance. It is an offence under the *Invasion of Privacy Act 1971* to use a listening device to overhear, record, monitor or listen to a private conversation, of which you are not party to.[37] Certain exceptions apply, including if you are party to a private conversation. Further regulations apply regarding the publishing or communication of any recordings.[38]

- *Information Privacy Act 2009* (Qld)

The *Information Privacy Act* only applies to Queensland Government agencies and does not cover actions by individual citizens, private sector organisations or the community sector. Residential care service providers should refer to Commonwealth privacy legislation, including the *Privacy Act 1988* and the Australian Privacy Principles.

- *Criminal Code 1899* (Qld)

Providers should also note the Queensland *Criminal Code* which provides for misdemeanour where a person observes or visually records another person 'in circumstances where a reasonable adult would expect to be afforded privacy', if the second person is in a private place or engaged in a private act and has not provided consent.[39]

For **residential aged care facilities,** the regulation of surveillance devices in Queensland legislation is relatively limited and therefore providers should take note of the Commonwealth privacy legislation, the *Privacy Act 1988* and the *Charter of Aged Care Rights.*

---

35 Surveillance Devices Act 2007 (NT) ss 11, 12, 13.
[36] *Surveillance Devices Act 2007* (NT) s 39.
[37] *Invasion of Privacy Act 1971* (Qld) s 43(1).
[38] *Invasion of Privacy Act 1971* (Qld) s 45.
[39] *Criminal Code 1899* (Qld) s 227A.

South Australia

Relevant legislation: *Surveillance Devices Act 2016* (SA), *Summary Offences Act 1953* (SA)

- *Surveillance Devices Act 2016* (SA)

The key piece of legislation governing surveillance devices is the *Surveillance Devices Act 2016.* Under this Act, a person must not install, use or maintain a surveillance device to record or visually observe the carrying on of a private activity **without the express or implied consent of each party to the activity.**[40] Activities in resident's bedroom almost certainly falls under the category of 'private activities', meaning that consent of all recorded parties is required – this could include staff, visitors and other residents.

Certain exceptions may apply, including where operation of the device is authorised under another law, or where it is used as part of an approved undercover operation.[41]

- *Summary Offences Act 1953* (SA)

Use of optical surveillance devices for the purpose of filming or distributing invasive or indecent footage constitutes an offence under the *Summary Offences Act 1953* (SA).[42]

Western Australia

Relevant legislation: *Surveillance Devices Act 1998* (WA)

It is an offence under the *Surveillance Devices Act 1998* to install, use or maintain: (i) listening devices to record or listen to a private conversation; or (ii) optical surveillance devices to record visually or observe a private activity, in circumstances where not **all of the principal parties** to the private conversation or activity have given their consent to be recorded, observed or listened to.[43] The Act also regulates the use of tracking devices in respect of the location of persons and objects.

Activities recorded by a camera installed in a client's bedroom may be considered a private activity as it occurs in a private area where parties would not ordinarily be observed.

Certain exceptions may apply, including where operation of the device is authorised as part of a criminal investigation, or where it is reasonably necessary to protect the lawful interests of the principal party.[44]

Tasmania

Relevant legislation: *Listening Devices Act 1991* (Tas), *Personal Information Protection Act 2004* (Tas), *Police Offences Act 1935* (Tas)

- *Listening Devices Act 1991* (Tas)

In Tasmania, *the Listening Devices Act 1991* restricts the use of listening devices. It does not address the regulation of optical surveillance devices. Under this Act it is an offence to use a listening device to record or listen to a private conversation.[45]

- *Personal Information Protection Act 2004* (Tas)

Publicly operated providers and providers who have entered into a personal information contract with a government agency should also be aware of the *Personal Information Protection Act 2004*, which creates further obligations with regard to the collection, use and disclosure of personal information obtained by the organisation.

---

[40] *Surveillance Devices Act 2016* (SA) s 5(1).
41 Surveillance Devices Act 2016 (SA) s 6(1).
42 Summary Offences Act 1953 (SA) ss 26B, 26C & 26D.
43 See Surveillance Devices Act 1998 (WA) ss 3 & 6.
44 Surveillance Devices Act 1998 (WA) s 6(3).
45 See Listening Devices Act 1991 (Tas) ss 3, 5 & 12.

- *Police Offences Act 1935* (Tas)

Use of optical surveillance devices in certain circumstances can constitute a criminal offence under Tasmania's *Police Offences Act 1935* (Tas). Under the *Act,* it as offence for a person to observe or visually record another person without their consent, in circumstances where a person would expect to be afforded privacy, and where the person is in a private place or engaged in a private act.[46]

- End of document -

Disclaimer: This resource has been developed by BNG as a starting point for your organisation and should be tailored according to the organisation's service type(s) and specific requirements. BNG has made every attempt to ensure the accuracy and currency of this information, however it is not intended to be comprehensive nor does it constitute legal advice.

46 Police Offences Act 1935 (Tas) s13A.