

Physical security systems policy

Purpose and Scope

Ahpra is committed to providing and maintaining a safe and healthy workplace for all Workers. This policy outlines the process, standards and rules Ahpra adopts for the appropriate management and operation of Ahpra's Physical Security Systems, including:

- Closed Circuit Television (**CCTV**), and
- the Electronic Access Control System (**EACS**).

This policy also outlines how Ahpra collects, uses, discloses and destroys CCTV Footage and EACS Data.

All capitalised terms are as defined at the end of the Policy in the Definitions. Where a term is not defined the ordinary general meaning of the term should apply.

Coverage

This policy applies to all Workers and Visitors.

Policy

1. Principles

1.1 Ahpra uses workplace CCTV and EACS to:

- provide protection to Workers who may be vulnerable to a Security Incident in public areas, such as the reception area,
- view a live Security Incident as it is occurring to enable a quick, appropriate response,
- deter and capture Security Incidents including theft, vandalism, violence, unauthorised access, malicious behaviour or misconduct,
- audit CCTV Footage and EACS Data to enable the identification, analysis, verification and evaluation of Security Incidents to support an evidence-based response,
- to undertake disciplinary action for identified Security Incidents, and
- review Security Incidents by storing data and facilitate investigations, if required.

2. Ethical use of Physical Security Systems

2.1 Authorised Users, as defined by this policy, are required to:

- comply with the legislative requirements in each State and Territory and the *Privacy Act 1988 (Cth)* (**Privacy Act**) when collecting, reviewing, and disclosing CCTV Footage or EACS Data,
- prevent any abuse / misuse of CCTV Footage or EACS Data in accordance with applicable Ahpra [IT security policies](#),
- respond to law enforcement agencies and Ahpra's National Executive in a timely and professional manner in the event of a Security Incident or investigation,
- ensure confidentiality of data gathered through CCTV or EACS operations by not disclosing or discussing contents with unauthorised persons who have no direct responsibility relating to CCTV or EACS operations, and

178113:23915618_1 Australian Health Practitioner Regulation Agency
National Boards

GPO Box 9958 Melbourne VIC 3001 Ahpra.gov.au 1300 419 495

Ahpra and the National Boards regulate these registered health professions: Aboriginal and Torres Strait Islander health practice, Chinese medicine, chiropractic, dental, medical, medical radiation practice, midwifery, nursing, occupational therapy, optometry, osteopathy, paramedicine, pharmacy, physiotherapy, podiatry and psychology.

- use CCTV Footage and EACS Data only for its intended purpose, outlined above, and not for personal benefit or an alternative purpose.
- 2.2 A Worker requesting access to Ahpra's Physical Security Systems that has a valid reason (including security system equipment or data) who's access is approved must first acknowledge that they have received, understood and agree to comply with this policy before access is permitted.

3. CCTV camera monitoring

- 3.1 CCTV cameras in Ahpra's offices will only be installed:
- in compliance with the relevant jurisdictional surveillance and privacy legislation following a review of the proposed location and terms of operation by Corporate Legal
 - with the written approval of the Executive Director of People and Culture following Corporate Legal's review, and
 - in accordance with this policy.
- 3.2 Ahpra will ensure that its CCTV system is configured to record video images only and will not record audio.
- 3.3 Where Ahpra proposes to install or modify a CCTV system in one of its offices, Workers will be provided with at least **30 days' notice** following a period of consultation. The notice will include a floorplan with locations of cameras, technical specifications of equipment being installed, date of installation of equipment, the date of the commencement of CCTV recording, details for an Ahpra contact person and any other information required under state and territory surveillance legislation for any enquiries.
- 3.4 Newly commencing Workers will be given notice of the operation of CCTV at the earliest possible opportunity, either prior to commencing or during induction, and in accordance with the relevant state or territory requirements.
- 3.5 In implementing CCTV, Ahpra will ensure that:
- cameras, their casings and other associated equipment that would indicate the presence of CCTV are visible,
 - signs are displayed at each camera location to advise that the area is under CCTV monitoring, and
 - Workers and Visitors are notified about the existence of a CCTV system.
- 3.6 For the purposes of ensuring safety and security of Workers, Ahpra will use a live feed of CCTV cameras in public areas of its offices (i.e. reception areas). This live feed shall be visible on monitors located at duress strobes in the secure back-of-house area and used specifically in duress situations to facilitate an immediate and effective response.

4. Access, storage and retention

- 4.1 CCTV Footage will be retained for a minimum of 30 days and a maximum of 90 days. This may be extended where a Security Incident has occurred or where required to conduct an investigation. No backup is held of CCTV images.
- 4.2 EACS Data will be retained for a period of 7 years in accordance with the Retention and Disposal Authority for Administrative Records of National Bodies.
- 4.3 CCTV Footage and EACS Data must not be copied or taken from Ahpra's Physical Security Systems without an approved application in the form of Schedule 1.
- 4.4 CCTV Footage and EACS Data will be deleted after the relevant retention period.
- 4.5 Ahpra will maintain appropriate security measures and audit trails against unauthorised access, alteration, disclosure, accidental loss or inadvertent destruction of CCTV Footage and EACS Data.

5. Review and disclose/release CCTV and EACS Data

- 5.1 Requests for review or disclosure/release of CCTV Footage and EACS Data must be submitted in an approved application in the form of Schedule 1 to the Property and Physical Security Manager.
- 5.2 CCTV Footage and EACS Data may only be approved for review or disclosure by the Executive Director, People and Culture or the National Director, Employee Services in accordance with the Ahpra physical security framework, if it meets **one or more** of the following criteria:
- is required by an enforcement agency in relation to an offence,
 - is related to civil or criminal proceedings,
 - is reasonably believed necessary to avert an imminent threat of serious violence to persons or substantial damage to property,
 - is an approved request in relation to an ongoing investigation pertaining to a Security Incident, alleged misconduct, or serious misconduct, and/or
 - the requestor has a right under the Privacy Act or applicable legislation for that relevant state or territory.

Third party requests

- 5.3 All requests for third party access, with the exception of law enforcement agencies, for CCTV Footage or EACS Data must be made in writing to:

Property and Physical Security Manager
Ahpra
GPO Box 9958
Adelaide SA 5001
Email: Physical.Security@ahpra.gov.au

- 5.4 When assessing a request for access, all applicable legislation will be considered and assessed, including the requirements set out in clause 5.2 above. If a request for access is approved, Ahpra will:
- only disclose information relevant to the third party's request; and
 - take all reasonable steps to de-identify individuals in footage if they are not relevant for the purposes of disclosure.

6. Records Disposal

- 6.1 CCTV Footage and EACS Data that was retained due to a request for disclosure is classified as confidential and must be disposed of in accordance with [Ahpra's Information storage and disposal policy](#), the Privacy Act and any applicable state or territory specific legislation.

7. Complaints handling

- 7.1 Enquiries regarding the purpose, use or other aspects of Ahpra's Physical Security Systems should be directed to:

Property and Physical Security Manager
Ahpra
GPO Box 9958
Adelaide SA 5001
Email: Physical.Security@ahpra.gov.au

- 7.2 All complaints will be handled in accordance with [Ahpra's workplace complaints and reporting procedure](#) to ensure fairness, consistency and timely resolution.
- 7.3 If an individual is not satisfied with how their complaint is handled under clause 7.2, individuals also have the right to make a complaint to the relevant authority in their state or territory or the National Health Practitioner Privacy Commissioner, who is also the [National Health Practitioner Ombudsman](#). Please see the office's contract details below.

Contact Details

Phone: 1300 795 265 (a translating and interpreting service is available via 131 450)

Office hours are 9:00 am to 5:00 pm AEST, Monday to Friday (excluding public Holidays). A voicemail service is also available.

Online complaint form: <https://www.nhpo.gov.au/make-a-complaint-to-the-commissioner>

Email: complaints@NHPO.gov.au

Post: National Health Practitioner Ombudsman, GPO Box 2630, Melbourne, Victoria, 3001

8. Non-compliance with this policy

- 8.1 Security operations require high standards of integrity, honesty and to abide by legislation. Workers are required to report any breaches immediately to their manager and through Log It.
- 8.2 When behaviour warrants investigation and a person is found to have acted in contravention of the physical security framework or inappropriately/unlawfully, the matter is to be handled in accordance with [Ahpra's Code of Conduct](#) and [Discipline policy](#).

Ahpra Related documents

- Ahpra Physical security access control policy *[currently being drafted]*
- [Ahpra Information storage and disposal policy](#),
- [Ahpra Code of Conduct](#)
- [Ahpra Discipline Policy](#)
- [Office visitor security procedure](#) *[currently being updated]*
- [Ahpra's workplace complaints and reporting procedure](#)

Public Related documents

- [Protective Security Policy Framework](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Surveillance Devices Act 1999 \(VIC\)](#)[Surveillance Devices Act 2016 \(SA\)](#)
- [Surveillance Devices Act 1998 \(WA\)](#)
- [Surveillance Devices Act 2007 \(NT\)](#)
- [Workplace Privacy Act 2011 \(ACT\)](#)
- [Workplace Surveillance Act 2005 \(NSW\)](#)

Definitions

Term	Definition
Authorised User	Workers who have been explicitly authorised by the Executive Director, People and Culture or the National Director, Employee Services to access, review, view or disclose CCTV Footage and/or EACS Data. These Workers will include the Property and Physical Security Manager, the Facilities Manager and other Workers as may be authorised from time to time.
CCTV Footage	Images captured by the CCTV system and the metadata that is integral to establishing the context and authenticity of the footage.

Term	Definition
Contingent Worker	An individual or groups of workers hired by Ahpra from a third-party recruitment agency supplier or as an individual contractor, to provide labour or services.
EACS	Ahpra's electronic security card system which manages and regulates who can enter or exit secure areas of Ahpra's offices using electronic methods such as card readers, access cards and software.
EACS Data	Data collected by and stored in Ahpra's EACS.
Physical Security Systems	Ahpra's CCTV and EACS.
Security Incident	An event that compromises the safety and security of Ahpra's physical assets, information, Workers and/or Visitors. This can include unauthorised access to areas within or to Ahpra's office, theft or damage of equipment, break-ins, vandalism, physical assaults, or any other situation that threatens the physical integrity of Ahpra's property or the safety of its Workers and/or Visitors.
Worker	A person who carries out work for Ahpra, including: the National Executive, employees, contractors and Contingent Workers, volunteers, interns, work experience staff and statutory appointees (board, committee, and panel members).
Visitors	A person who is not a worker issued with a permanent ID access card who is attending an Ahpra workplace for any purpose (i.e a member of the general public, delivery person (including catering or trade contractor).

Document control	
Approval authority	National Executive
Policy Owner (administrative)	Executive Director People and Culture
Responsible Officer	National Director, Employee Services
Approval date	11 September 2024
Start date	26 September 2024
Next review due date	26 September 2027

Schedule 1 – Requests for CCTV Footage and/or EACS Data



Request for Closed-Circuit Television (CCTV) and Electronic Access Control System (EACS) data

Requester	Name				
	Position				
	Contact number				
	Email address				
	Signature				
Date request lodged				Log It Reference	
Request Details:					
Type of request		☐ Authorised user to view EACS data and provide report. ☐ Copy of EACS data. ☐ Authorised user to view CCTV footage and provide report. ☐ Copy of CCTV footage.			
Date(s) of incident		Start Time		Finish Time	
Reason for request (e.g. the nature and description of incident)					
Are staff, statutory appointees, contractors or the public likely to be captured on footage?		☐ Yes ☐ No	People likely to be identified: ☐ Ahpra Staff ☐ Statutory appointees ☐ Contractors / Public	De-identification required: ☐ Yes ☐ No	
If requesting CCTV footage, please describe the incident or scenario and reason for access. (This will assist the CCTV authorised user to recover the footage from the correct camera.)					
Please highlight the area listed below that relates you to your request					
Ahpra CCTV cameras				Building owners CCTV cameras	
Front-of-House Entry Door		Back-of-House Entry Door		Ground floor foyer	
Reception Area		Evidence Room		Goods lift	
IT Communications Room		All cameras		Lift Foyer - Ahpra floor	
Authoriser	Name				
	Position				
	Signature				

Australian Health Practitioner Regulation Agency
National Boards

GPO Box 9958 Melbourne VIC 3001 Ahpra.gov.au 1300 419 495

Ahpra and the National Boards regulate these registered health professions: Aboriginal and Torres Strait Islander health practice, Chinese medicine, chiropractic, dental, medical, medical radiation practice, midwifery, nursing, occupational therapy, optometry, osteopathy, paramedicine, pharmacy, physiotherapy, podiatry and psychology.