My Health Records (Information Commissioner Enforcement Powers) Guidelines 2026

My Health Records Act 2012

I, **ELIZABETH TYDD**, Australian Information Commissioner, make this legislative instrument under subsection 111(2) of the *My Health Records Act 2012*.

Dated

ELIZABETH TYDD **DRAFT ONLY—NOT FOR SIGNATURE**
Australian Information Commissioner

Contents

Part 1 Preliminary

1 Name of instrument

This instrument is the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2026.*

2 Commencement

2.1 This instrument takes effect on the day following the day of its registration in the Federal Register of Legislation maintained under section 15A of the *Legislation Act 2003*.

2.2 The *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* is repealed when the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2026* commences.

> *Note: Section 33(3) of the Acts Interpretation Act 1901 (Cth) provides that when an Act confers a power to make, grant or issue an instrument of a legislative or administrative character, the power shall be construed as including a power to repeal, rescind, revoke, amend or vary any such instrument.*

2.3 From the date of commencement, the Information Commissioner will have regard to this instrument when exercising enforcement powers or investigative powers under both the *My Health Records Act 2012* (My Health Records Act) and the *Privacy Act 1988* (Privacy Act), in relation to the My Health Record system.

3 Definitions

3.1 Unless the contrary intention appears, terms used in these guidelines have the same meaning as in the My Health Records Act.

3.2 In this instrument:

agency has the same meaning as in section 6 of the Privacy Act.

AIC Act means the *Australian Information Commissioner Act 2010*.

Commissioner initiated investigation is an investigation initiated by the Information Commissioner under subsection 40(2) of the Privacy Act.

Court means:

(a) the Federal Court of Australia;
(b) the Federal Circuit and Family Court of Australia (Division 2) of Australia; or
(c) a court of a State or Territory that has jurisdiction in relation to matters arising under the My Health Records Act.

Information Commissioner means the person appointed as Australian Information Commissioner under subsection 14(1) of the AIC Act, or under subsection 21(1) of that Act.

Note: For acting appointments, section 33A of the Acts Interpretation Act 1901 also applies.

My Health Record means the My Health Record as defined in section 5 of the My Health Records Act.

My Health Records Act means the *My Health Records Act 2012*.

My Health Records Rules means rules made under section 109 of the My Health Records Act.

My Health Record system means the electronic health record system established under the My Health Records Act, and as defined in section 5 of that Act.

National Repositories Service means the National Repositories Service referred to in paragraph 15(i) of the My Health Records Act.

participant in the My Health Record system means any of the following:

(a) the System Operator;
(b) a registered healthcare provider organisation;
(c) the operator of the National Repositories Service;
(d) a registered repository operator;
(e) a registered portal operator; or
(f) a registered contracted service provider, so far as the contracted service provider provides services to a registered healthcare provider.

Privacy Act means the *Privacy Act 1988*.

registered repository operator means a person that:

(a) holds, or can hold, records of information included in My Health Records for the purposes of the My Health Record system; and
(b) is registered as a repository operator under section 49 of the My Health Records Act.

Regulatory Powers Act means the *Regulatory Powers (Standard Provisions) Act 2014.*

SES means Senior Executive Service as defined by section 35 of the Public Service Act.

System Operator has the meaning given by section 14 of the My Health Records Act.

4 Introduction

The Information Commissioner

4.1 The Information Commissioner is a statutory office holder appointed by the Governor-General under subsection 14(1) of the AIC Act. The Information Commissioner performs functions and exercises powers conferred on the Information Commissioner by the AIC Act and other Acts.

4.2 The My Health Records Act and the Privacy Act both confer functions and powers on the Information Commissioner in relation to the My Health Record system.

Overview of the My Health Record system

4.3 The My Health Record system is established under and is regulated by the My Health Records Act. The My Health Record system aims to enable the secure sharing of health information between a healthcare recipient's registered healthcare provider organisations, while enabling the healthcare recipient to control who can access their My Health Record. The My Health Records Act establishes the role and function of the System Operator, a registration framework for recipients and participants in the My Health Records system, and a privacy framework.

4.4 The System Operator is responsible for the operation of the My Health Record system. This includes, but is not limited to, the operation of the National Repositories Service that stores key records that form part of a registered healthcare recipient's My Health Record and associated index services and access control mechanisms.

Regulation of health information

4.5 The My Health Records Act and regulations and rules made under that Act regulate the collection, use and disclosure of health information contained in a healthcare recipient's My Health Record.

4.6 In addition to the requirements in the My Health Records Act, the System Operator is subject to the Privacy Act.

4.7 In addition to the requirements in the My Health Records Act, other participants in the My Health Record system are subject to the Privacy Act and relevant State and Territory privacy laws.

Functions of the Information Commissioner in relation to My Health Record System

4.8 The Information Commissioner's functions in the My Health Record system under the My Health Records Act are:

a) investigating an act or practice that may be an interference with the privacy of a healthcare recipient under subsection 73(1), and, if the Information Commissioner considers it appropriate to do so, attempting by conciliation to effect a settlement of the matters that gave rise to the investigation;

b) receiving data breach notifications (section 75);

c) accepting and enforcing undertakings relating to compliance (section 80)

d) seeking injunctions to restrain a person from contravening a provision, or to compel compliance with a provision (section 81);

e) enforcing civil penalties (section 79);

f) formulating guidelines relating to the Information Commissioner's enforcement powers (section 111); and

g) sharing details of investigations with the System Operator if satisfied this would enable the Systems Operator to monitor or improve the operation or security of the My Health Record system (section 73A).

The role of these guidelines

4.9 Section 111 of the My Health Records Act requires the Information Commissioner to formulate, and have regard to, guidelines regarding the exercise of the Information Commissioner's powers under the My Health Records Act or a power under another Act that is related to such a power. The Privacy Act is a related Act.

4.10 While these guidelines seek to provide guidance to participants in the My Health Record system, the Information Commissioner has a discretion to exercise the available powers that he or she considers most appropriate in the particular circumstances of each case.

Part 2 General principles relating to complaints handling, the exercise of investigative powers, and enforcement action

5 Types of investigative and enforcement powers available to the Information Commissioner

5.1 The Information Commissioner has a range of enforcement powers and investigative powers under both the My Health Records Act and the Privacy Act in relation to the My Health Record system. The Information Commissioner also has information sharing powers that may be used for the purposes of exercising enforcement and investigation powers and performing functions or duties under the Privacy Act.

General approach to complaints

5.2 APP 1 outlines the requirements for an APP entity to manage personal information in an open and transparent way. APP 1 imposes obligations upon an APP entity to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and is able to deal with related inquiries and complaints (APP 1.2).

5.3 A complaint received by the Information Commissioner relating to the My Health Record system will, unless there is a reason to accept the complaint and act under the My Health Records Act, be treated as a complaint made under section 36 of the Privacy Act, and may be dealt with under the provisions of Part V and Part VIB of the Privacy Act. If a complaint is made under the Privacy Act, any regulatory action will be in accordance with the Privacy Act.

5.4 When investigating a complaint relating to the My Health Record system under the Privacy Act, the Information Commissioner may seek efficient and early dispute resolution by requesting that the complainant lodge their complaint with the My Health Record participant, and requesting that the participant take reasonable steps to resolve the complaint.

5.5 If early resolution or conciliation is not possible, or if it is not reasonable for an individual to lodge a complaint with the My Health Record participant, the Information Commissioner may decide to investigate the complaint and may decide to take enforcement action under the My Health Records Act or the Privacy Act.

Investigative powers

5.6 The Information Commissioner has power under subsection 73(4) of the My Health Records Act to do all things necessary or convenient to investigate an alleged contravention of the My Health Records Act in relation to the My Health Record system, either in connection with health information in a healthcare recipient's digital record or as a result of a breach of a civil penalty provision.

5.7 As a contravention of the My Health Records Act in connection with health information included in a healthcare recipient's digital record or a provision of Part 4 or 5 is an interference with privacy for the purposes of the Privacy Act, the Information Commissioner may investigate the act or practice under the Privacy Act.

5.8 Part V of the Privacy Act sets out the investigative powers and processes available when the Information Commissioner conducts an investigation under the Privacy Act into an alleged interference with privacy.

5.9 The range of powers given to the Information Commissioner under Part V of the Privacy Act in relation to the conduct of investigations include powers to:

a) investigate a matter following a complaint or on the Commissioner's own initiative;

b) attempt to conciliate a complaint;

c) conduct preliminary inquiries to determine whether or not to open an investigation;

d) require information or a document to be produced;

e) require a person to attend before the Commissioner to answer questions under oath or affirmation;

f) enter premises to examine documents;

g) in certain circumstances, to hold a hearing, examine witnesses or call compulsory conferences; and

h) Part V also provides detail on how an investigation should be conducted, including procedural elements.

5.10 The Information Commissioner also has the ability to issue a monitoring or investigation warrant when investigating an offence provision or civil penalty provision in the Privacy Act, or a civil penalty provision enforceable by the Commissioner under the My Health Records Act. These powers are contained in Part VIB of the Privacy Act, and cannot be exercised without consent being given to the entry to the premises, or prior judicial authorisation in the form of a warrant. The Information Commissioner is subject to conditions when issuing a warrant to ensure that their use is not arbitrary, but reasonable and proportionate in the circumstances.

Enforcement powers

5.11 The Information Commissioner has enforcement powers under the My Health Records Act and Privacy Act, outlined in Part 3, which trigger specified parts of the Regulatory Powers Act and include:

a) enforceable undertakings (see section 8);

b) determinations (see section 9);

c) injunctions (see section 10);

d) civil penalties (see section 11);

e) compliance notices (see section 12); and

f) infringement notices (see section 13).

5.12 The Information Commissioner may also refer matters, when appropriate, to other complaint bodies or, in more serious cases, to law enforcement (see section 14).

6 Consistent regulatory approach

6.1 When performing functions or exercising complaint handling, investigation, or enforcement powers in relation to the My Health Record system, the Information Commissioner will:

(a) act consistently with the Commissioner's privacy regulatory approach under the Privacy Act;

(b) have regard to the Commissioner's and the OAIC's relevant policies for complaint handling, investigations, and enforcement action, as are in force from time-to-time and are publicly available; and

(c) have regard to its internal complaints handling and investigatory procedures.

Note: When investigating an alleged contravention and deciding whether to take enforcement action (see section 7), the Information Commissioner will act consistently with general principles of good decision making. This may involve having regard to the *Best Practice Guides* published by the Administrative Review Council.

General approach to Commissioner initiated investigations

6.2 Under s 40 of the Privacy Act, the Information Commissioner may, on his or her own initiative, decide to investigate an act or practice that may be an interference with the privacy of an individual.

6.3 A Commissioner initiated investigation relating to the My Health Record system will be conducted under Part V of the Privacy Act rather than under the My Health Records Act, unless there is a reason to conduct the investigation under the latter Act.

6.4 Following a Commissioner initiated investigation under the Privacy Act, the Information Commissioner may decide to take enforcement action under the Privacy Act or the My Health Records Act.

General approach to conducting investigations under section 73 of the My Health Records Act

6.5 Where the Information Commissioner decides to investigate under section 73 of the My Health Record Act (as an alternative to an investigation under Part V of the Privacy Act), the Commissioner will follow a process that, so far as practicable, corresponds with the investigative processes set out in Part V of the Privacy Act.

6.6 Upon completing an investigation under section 73 of the My Health Records Act, the Information Commissioner may take enforcement action under that Act.

7 Enforcement action – general principles

7.1 Factors the Information Commissioner may take into account in deciding whether to take enforcement action against a person in relation to the My Health Record system and what action to take, include the following:

a) the object of the My Health Records Act;

b) the objects of the Privacy Act;

c) whether the investigation was completed under the My Health Records Act or the Privacy Act;

d) any factors contained in policies on regulatory action set out by the Information Commissioner's office, such as:

i. whether there is a risk of substantial harm to individuals and the community, especially to vulnerable people and groups;

ii. whether the issues concern systemic harms or contraventions;

iii. whether action by the OAIC is likely to change sectoral or market practices, or have an educative or deterrent effect;

iv. whether the issues are subject to significant public interest or concern;

v. whether action by the OAIC will help clarify aspects of policy or law, especially newer provisions of the Acts administered by the OAIC;

e) any other factors which the OAIC considers relevant in the circumstances, including factors which are relevant to the specific regulatory power being used.

7.2 It is open to the Information Commissioner to use a combination of enforcement powers to address a particular contravention.

Administrative action of the System Operator

7.3 Section 73A of the My Health Records Act authorises the Information Commissioner to disclose to the System Operator any information or documents that relate to an investigation that the Information Commissioner conducts because of the operation of section 73 of that Act, if the Information Commissioner is satisfied that to do so will enable the System Operator to monitor or improve the operation or security of the My Health Record system.

7.4 A disclosure under section 73A of the My Health Records Act may also assist the System Operator in exercising the power to cancel, suspend or vary a person's registration with the My Health Record system in certain circumstances in accordance with the My Health Records Act.

General litigation principle

7.5 In any litigation, the Information Commissioner will act in accordance with the Commonwealth's model litigant obligations.

Publication of use of enforcement powers

7.6 The Information Commissioner may communicate publicly information about his or her use of enforcement powers under the Privacy Act or My Health Records Act. Exceptions may apply when a matter is referred to a law enforcement body for criminal investigation.

7.7 In relation to enforceable undertakings accepted under section 80V of the Privacy Act or section 80 of the My Health Records Act, the Information Commissioner will generally publish accepted enforceable undertakings.

Part 3 Use of enforcement powers

8 Enforceable undertakings

8.1 Under section 80 of the My Health Records Act, the Information Commissioner may accept a written undertaking by an entity, in relation to the My Health Records Act, given by a person that the person will comply with the My Health Records Act or to avoid contravening the My Health Records Act.

8.2 Under section 80V of the Privacy Act, the Information Commissioner may accept a written undertaking given by an entity to comply with the Privacy Act or avoid contravening the Privacy Act.

8.3 Both section 80 of the My Health Records Act and section 80V of the Privacy Act triggers the provisions of Part 6 of the Regulatory Powers Act which deals with the acceptance and enforcement of undertakings relating to compliance with legislative provisions.

8.4 The individual giving and executing the undertaking must have the authority to negotiate on behalf of, and bind, the respondent person.

8.5 The My Health Records Act and the Privacy Act do not impose a particular structure for an enforceable undertaking. However, an undertaking must be written and must be expressed to be an undertaking under s 114 of the Regulatory Powers Act.

9 Determinations

9.1 After investigating a complaint under section 36 of the Privacy Act, and as outlined in section 5 of these guidelines, the Commissioner may make a determination under section 52 of that Act which dismisses the complaint or finds that the complaint is substantiated.

9.2 The Commissioner can also make a determination after conducting an investigation on his or her own initiative.

9.3 Under Part V of the Privacy Act, the Information Commissioner may apply to a Court for an order to enforce a determination against a person or entity, or against an agency.

9.4 Following an investigation of a complaint or an investigation on the Commissioner's own initiative, the Information Commissioner has a discretion to make a determination within the prescriptions set out in the Privacy Act.

9.5 Where a respondent has failed to comply with the terms of a determination made under section 52 of the Privacy Act, the Information Commissioner will consider whether to commence proceedings in a Court to enforce the determination.

9.6 When deciding whether to commence proceedings to enforce a determination, the Information Commissioner may take into account:

a) the particular facts of the matter;

b) the factors referred to at section 7.1 of these guidelines; and

c) the Commonwealth's model litigant obligations referred to at section 7.5 of these guidelines.

10 Injunctions

10.1 Under section 81 of the My Health Records Act, which triggers Part 7 of the Regulatory Powers Act, the Information Commissioner may apply to a Court for an injunction to require a person to do, or to restrain a person from doing, specified actions.

10.2 Under section 80W of the Privacy Act, which triggers Part 7 of the Regulatory Powers Act, the Information Commissioner or any other person may apply to Court for an injunction to require a person to do, or to restrain a person from doing, specified actions.

10.3 When deciding whether to seek an injunction from a Court, the Information Commissioner may consider:

a) the particular facts of the matter;

b) the factors referred to at section 7.1; and

c) the Commonwealth's model litigant obligations referred to at section 7.5.

11 Civil penalties

11.1 Civil penalty provisions in the My Health Records Act that are within the remit of the Information Commissioner are provided in s 79 of the My Health Records Act. The Information Commissioner must make the application within four years of the alleged contravention.

11.2 Section 79 of the My Health Records Act and section 80U of the Privacy Act trigger the provisions of Part 4 of the Regulatory Powers Act which deals with seeking and obtaining a civil penalty order for contraventions of civil penalty provisions.

11.3 A contravention of the My Health Records Act in connection with health information included in a healthcare recipient's My Health Record or a provision of Part 4 or 5 is an interference with privacy for the purposes of the Privacy Act. Sections 13G and 13H of the Privacy Act, relating to serious interferences with privacy and interferences with privacy respectively, are civil penalty provisions.

11.4 Therefore, particular conduct may contravene both a civil penalty provision in the My Health Records Act and the 'serious interference with privacy' or 'interference with privacy' civil penalty provisions in the Privacy Act. In these circumstances, the Information Commissioner may decide to seek a civil penalty under the Privacy Act for an interference with privacy arising from a contravention of the My Health Records Act.

11.5 A civil penalty order cannot be sought in relation to a contravention of the 'serious interference with privacy', 'interference with privacy', and compliance notice civil penalty provisions if the entity has already been issued with a compliance notice in relation to the same conduct and:

a) the notice has not been withdrawn and the entity has complied the notice; or

b) the entity applied to the Court for review of the notice and the application has not been completely dealt with.

12 Compliance notices

12.1 Under section 80UC of the Privacy Act, a compliance notice may be issued by the Information Commissioner, or a SES member of the staff of the Commissioner, if there is a reasonable belief that an entity has contravened a compliance notice provision. A compliance notice is a discretionary notice which may be issued to an entity before an infringement notice is issued. It is intended to provide an entity with practical and measurable steps it can take to comply with obligations outlined in compliance notice provisions.

12.2 Section 80UC of the Privacy Act prescribes the requirements for giving a valid compliance notice, the matters that must be outlined, requirements for entities to comply with a compliance notice, and the relationship and interaction of compliance notices with other enforcement powers.

13 Infringement notices

13.1 Under s 80UB of the Privacy Act, an infringement notice may be issued by the Information Commissioner, or a SES member of the staff of the Commissioner, where there is a reasonable belief that infringement notice provisions have been contravened. An infringement notice sets out the particulars of an alleged contravention of an offence or civil penalty provision and an amount to be paid. An entity that is issued with an infringement notice can choose to pay the penalty amount specified in the notice as an alternative to court proceedings.

13.2 Section 80UB of the Privacy Act with Part 5 of the Regulatory Powers Act prescribes the requirements for giving a valid infringement notice, including when an infringement notice may be given, the matters to be included in an infringement notice, how an extension of time to pay may be sought, and how a withdrawal of an infringement notice may be sought.

13.3 Subsection 80UC(10) of the Privacy Act and subsection 103(2) of the Regulatory Powers Act prescribe circumstances in which the Information Commissioner may not issue an infringement notice.

14 Referrals

14.1 The Privacy Act confers on the Information Commissioner a range of privacy regulatory powers, including powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

14.2 Where the OAIC receives a complaint, it may not always be the most appropriate body to investigate and resolve that complaint. It has various powers under the Privacy Act to decline to investigate where there is an alternative applicable law or complaint handling body (section 41), or to refer complaints to other complaint bodies in certain circumstances (section 50).

14.3 There are criminal offences under the My Health Records Act and Privacy Act. These enable the OAIC to refer matters to the Commonwealth Director of Public Prosecutions. For example, it is a criminal offence for a body corporate to repeatedly not comply with the requirement to give information, answer a question or produce a document or record under the Privacy Act (subsection 66(1AA) of that Act).

Note

1. All Acts, legislative instruments, notifiable instruments and compilations of the aforementioned are registered on the Federal Register of Legislation established under the *Legislation Act 2003.* See www.legislation.gov.au.