



My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016

My Health Records Act 2012

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

Dated 18 March 2016

TIMOTHY PILGRIM
Acting Australian Information Commissioner

Contents

Part 1	Preliminary	3
1	Name of instrument	3
2	Commencement	3
3	Definitions	3
4	Introduction	5
Part 2	General principles relating to enforcement action and the exercise of investigative powers under the My Health Records Act and the Privacy Act	7
5	Types of enforcement powers and investigative powers available to the Information Commissioner	7
6	Investigations – general principles	9
7	Enforcement action – general principles	10
Part 3	Use of enforcement powers under the My Health Records Act and Privacy Act	13
8	Enforceable undertakings under the My Health Records Act	13
9	Enforceable undertakings under the Privacy Act	15
10	Determinations under the Privacy Act	17
11	Injunctions under the My Health Records Act	19
12	Injunctions under the Privacy Act	19
13	Civil penalties under the My Health Records Act	20
14	Civil penalties under the Privacy Act	21

Part 1 Preliminary

1 Name of instrument

This instrument is the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*.

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 *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013* (Federal Register of Legislative Instruments No. F2013L01085) is repealed when this *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* commences.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 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 Court 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*.

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, or appointed pursuant to s 21(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 his or her My Health Record.
- 4.4 The My Health Record system is decentralised, with a healthcare recipient's health information held in repositories across multiple locations and able to be accessed online by the healthcare recipient and their registered healthcare provider organisation(s). The National Repositories Service holds key records about healthcare recipients, including the healthcare recipient's shared health summary (created by a nominated healthcare provider and uploaded to the National Repositories Service), discharge summaries, event summaries and healthcare recipient entered information.
- 4.5 Private and public sector bodies may also register as repository operators. When a registered healthcare provider organisation wishes to and is authorised to access a healthcare recipient's health information that is contained in a repository (other than the National Repositories Service), that information may be able to be called up and viewed by the healthcare provider organisation, although its location remains with the relevant public or private sector body repository. For example, a healthcare provider organisation can view a pathology report for a healthcare recipient that is located at a particular pathology lab, if that pathology lab is a registered repository operator.
- 4.6 The System Operator is responsible for the operation of the My Health Record system.

Regulation of health information

- 4.7 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.
- 4.8 In addition to the requirements in the My Health Records Act, the System Operator is subject to the Privacy Act.

- 4.9 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

- 4.10 The Information Commissioner's functions in the My Health Record system include investigating alleged contraventions of the My Health Records Act and seeking to address contraventions as appropriate through conciliation, education and enforcement action.
- 4.11 Alleged contraventions of the My Health Records Act may be brought to the Information Commissioner's attention by a range of avenues including:
- a) a complaint by an individual or other notification from an individual or a participant in the My Health Record system;
 - b) as the result of a data breach notification provided in accordance with section 75 of the My Health Records Act;
 - c) as a referral from another regulator in certain circumstances;
 - d) as a result of media reporting;
 - e) as a result of information provided by an informant;
 - f) as a result of information provided by a law enforcement agency;
 - g) as a result of information received from the My Health Record System Operator;
 - h) during the course of an assessment or investigation conducted by the Information Commissioner.

The role of these guidelines

- 4.12 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.
- 4.13 These guidelines are made under section 111 of the My Health Records Act. These guidelines set out the Information Commissioner's general approach to the exercise 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.
- 4.14 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 enforcement action and the exercise of investigative powers under the My Health Records Act and the Privacy Act**

5 Types of enforcement powers and investigative 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. These powers are based on an escalation model. The general approach the Information Commissioner will take when determining which Act to apply is set out in sections 6 and 7 of these guidelines.

Investigative powers under the My Health Records Act

5.2 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. The civil penalty provisions in the My Health Records Act are listed below at section 13.3 of these guidelines.

Investigative powers under the Privacy Act

5.3 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.

5.4 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.

- 5.5 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 investigate a matter following a complaint or on the Commissioner's own initiative, attempt to conciliate a complaint, conduct preliminary inquiries to determine whether or not to open an investigation, require information or a document to be produced, require a person to attend before the Commissioner to answer questions under oath or affirmation, enter premises to examine documents and, in certain circumstances, to hold a hearing, examine witnesses or call compulsory conferences. Part V also provides detail on how an investigation should be conducted, including procedural elements.

Enforcement powers under the My Health Records Act

- 5.6 The Information Commissioner has enforcement powers under the My Health Records Act (which triggers specified parts of the Regulatory Powers Act). These powers include the ability to do one or more of the following:
- a) accept an enforceable undertaking;
 - b) apply to a Court for an order to enforce an enforceable undertaking ;
 - c) apply to a Court for an injunction to require a person to do, or to restrain a person from doing, specified actions;
 - d) apply to a Court for an order that a person who is alleged to have contravened a civil penalty provision in the My Health Records Act pay the Commonwealth a pecuniary penalty.
- 5.7 The Information Commissioner's use of each of these enforcement powers is discussed below at section 8 (enforceable undertakings), section 11 (injunctions) and section 13 (civil penalty orders).

Enforcement powers under the Privacy Act

- 5.8 The Information Commissioner has enforcement powers under the Privacy Act that include the ability to do one or more of the following:
- a) accept an enforceable undertaking
 - b) apply to the Federal Court or the Federal Circuit Court for an order to enforce an enforceable undertaking
 - c) make a non-binding determination;
 - d) apply to the Federal Court or the Federal Circuit Court for an order to enforce a determination;
 - e) apply to the Federal Court or the Federal Circuit Court for an injunction to require a person to do, or restrain a person from doing, specified actions

- f) apply to the Federal Court or the Federal Circuit Court for an order that a person who is alleged to have contravened a civil penalty provision in the Privacy Act pay the Commonwealth a pecuniary penalty.
- 5.9 The Information Commissioner's use of these enforcement powers is discussed below at section 9 (enforceable undertakings), section 10 (determinations), section 12 (injunctions) and section 14 (civil penalty orders).

6 Investigations – general principles

- 6.1 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, as explained in the *Best Practice Guides* published by the Administrative Review Council in 2007. In particular, the Information Commissioner will act fairly, transparently, and in accordance with principles of natural justice (or procedural fairness).

General approach to complaints

- 6.2 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 will be investigated under the provisions of Part V of the Privacy Act. If a complaint is made under the Privacy Act, any investigation must be in accordance with the Privacy Act.
- 6.3 When investigating a complaint relating to the My Health Record system under the Privacy Act, the Information Commissioner must make a reasonable attempt to conciliate the complaint. The Information Commissioner may decline to investigate or further investigate a complaint if there is no reasonable likelihood of a conciliated outcome. Following a complaint investigation, the Commissioner may decide to take enforcement action under the My Health Records Act or the Privacy Act.

General approach to Commissioner initiated investigations

- 6.4 The 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. The Commissioner may decide to commence a Commissioner initiated investigation following a complaint or data breach notification, or may commence a Commissioner initiated investigation independently of any complaint or notification.
- 6.5 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.

- 6.6 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

- 6.7 Where the Information Commissioner decides to conduct an investigation 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.
- 6.8 Upon completing an investigation under section 73 of the My Health Records Act, the Information Commissioner may take enforcement action under that Act. The Commissioner will consider the suitability of attempting by conciliation to effect a settlement of a matter under paragraph 73(3)(a) of the My Health Records Act before deciding to take enforcement action.

7 Enforcement action – general principles

Factors taken into account

- 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) the seriousness of the incident or conduct to be investigated, including:
 - i. the number of persons potentially affected;
 - ii. whether the matter involves sensitive information (as defined in s 6 of the Privacy Act) or other information of a sensitive nature;
 - iii. the adverse consequences caused or likely to be caused to one or more persons arising from an incident or conduct;
 - iv. whether disadvantaged or vulnerable groups may have been or may be particularly adversely affected or targeted;
 - v. whether conduct was deliberate or reckless;
 - vi. the seniority and level of experience of the person or persons responsible for the conduct;

- e) the level of public interest or concern relating to the conduct (with enforcement action more likely to be taken where significant public interest or concern exists);
- f) whether the burden on the individual or entity likely to arise from the enforcement action is justified by the risk posed to the protection of personal information;
- g) the specific and general educational, deterrent or precedential value of the particular enforcement action, including whether pursuing court action (where applicable) would test or clarify the law;
- h) whether the individual or entity responsible for the incident or conduct has been the subject of prior compliance or enforcement action in relation to the My Health Record system or by the Information Commissioner, and the outcome of that action;
- i) the likelihood of the individual or entity contravening the My Health Records Act or Privacy Act in the future;
- j) whether the conduct is an isolated instance, or whether it indicates a potential systemic issue (either with the individual or entity concerned or within an industry) or an increasing issue which may pose ongoing compliance or enforcement issues;
- k) action taken by the individual or entity to remedy and address the consequences of the conduct, including whether the individual or entity attempted to conceal a contravention or data breach, and whether the individual or entity has co-operated with the Information Commissioner during containment and any investigation of the contravention;
- l) whether the conduct has affected the security or integrity of the My Health Record system or impacted on healthcare provider or healthcare recipient confidence in the My Health Record system;
- m) the time since the conduct occurred;
- n) the cost and time required to achieve an appropriate remedy through enforcement action;
- o) whether there is adequate evidence available and admissible in a court to prove a contravention on the balance of probabilities;
- p) any other factors which the Information Commissioner 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 within the meaning under Appendix B of the *Legal Services Directions 2005*.

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.
- 7.7 In relation to enforceable undertakings accepted under s 33E of the Privacy Act or s 80 of the My Health Records Act, the Information Commissioner will generally publish accepted enforceable undertakings.
- 7.8 The Information Commissioner will publish determinations made under section 52 of the Privacy Act. The Commissioner will generally publish the name of the respondent. However, the Commissioner will generally not publish the names of complainants, respondent individuals or any third party individuals.

Part 3 Use of enforcement powers under the My Health Records Act and Privacy Act

8 Enforceable undertakings under the My Health Records Act

Legislative basis for accepting undertakings

- 8.1 Under section 80 of the My Health Records Act, the Information Commissioner may accept a written undertaking in relation to the My Health Records Act given by a person that the person will:
- a) take specified action in order to comply with the My Health Records Act;
 - b) refrain from taking specified action, in order to comply with the My Health Records Act; or
 - c) take specified action directed towards ensuring that the person does not contravene the My Health Records Act, or is unlikely to contravene the My Health Records Act, in the future.
- 8.2 Section 80 of the My Health Records 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.

Giving an enforceable undertaking

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

Terms of an undertaking

- 8.4 To be acceptable to the Information Commissioner, the terms of an enforceable undertaking should:
- a) describe the alleged contravention(s) about which the Information Commissioner is concerned;
 - b) outline specified steps the person will take to rectify the contravention, and ensure that it is not repeated or continued. This will usually include a requirement for the person to complete reviews and establish a monitoring and reporting framework;
 - c) contain dates by which the person is required to complete each step;
 - d) be capable of implementation and include action which is capable of being measured or tested objectively;
 - e) be certain and capable of enforcement.

- 8.5 The Information Commissioner will not accept an enforceable undertaking that:
- a) denies responsibility for an alleged contravention of the My Health Records Act or Privacy Act;
 - b) merely undertakes to comply with the law without explaining how compliance will be achieved;
 - c) seeks to impose terms or conditions on the Information Commissioner.

General approach to accepting undertakings

- 8.6 When deciding whether to accept an undertaking, the Information Commissioner may take into account:
- a) the particular circumstances of the matter;
 - b) the factors referred to at section 7.1 of these guidelines;
 - c) whether the Information Commissioner believes that the respondent has the ability to, and genuinely intends to, comply with the terms of the undertaking.

Withdrawing, varying or cancelling an undertaking accepted by the Information Commissioner

- 8.7 The person may withdraw or vary the undertaking at any time, but only with the written consent of the Information Commissioner.
- 8.8 The Information Commissioner may cancel the undertaking by written notice.
- 8.9 The Information Commissioner generally will only consent to the variation or withdrawal of an undertaking if:
- a) compliance with the enforceable undertaking is subsequently found to be impractical; or
 - b) there has been a material change in the circumstances which led to the undertaking being given, meaning that variation or withdrawal is appropriate in the circumstances; and
 - c) the Information Commissioner is satisfied that an appropriate regulatory outcome will still be achieved in the circumstances.

General approach to enforcing undertakings

- 8.10 If the Information Commissioner considers that a person has breached an undertaking accepted under section 80 and that undertaking has not been withdrawn or cancelled, the Information Commissioner may apply to a Court for one or more of the orders listed in that section:
- a) an order directing the person to comply with the undertaking;
 - b) an order directing the person to pay to the Commonwealth an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach;
 - c) any order that the Court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach;
 - d) any other order that the Court considers appropriate.
- 8.11 When deciding whether to seek an order from a Court to enforce an undertaking, the Information Commissioner may take into account:
- a) the particular circumstances of the matter;
 - b) the factors referred to at section 7.1 of these guidelines;
 - c) the Commonwealth's model litigant obligations referred to at section 7.5 of these guidelines.

9 Enforceable undertakings under the Privacy Act

- 9.1 Under section 33E of the Privacy Act, the Information Commissioner may accept a written undertaking given by an entity that an entity will:
- a) take specified action in order to comply with the Privacy Act;
 - b) refrain from taking specified action, in order to comply with the Privacy Act;
 - c) take specified action directed towards ensuring that the entity does not do an act, or engage in a practice, in the future that interferes with the privacy of an individual.

Giving an enforceable undertaking

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

Terms of an undertaking

- 9.3 For an undertaking to be acceptable to the Information Commissioner, it should include the terms listed at section 8.4 of these guidelines.

- 9.4 The Information Commissioner will not accept an enforceable undertaking under the Privacy Act that includes any of the terms listed at section 8.5 of these guidelines.

General approach to acceptance of an undertaking

- 9.5 In deciding whether to accept an undertaking under the Privacy Act, the Information Commissioner may consider those matters referred to in section 8.6 of these guidelines.

Withdrawing an undertaking accepted by the Information Commissioner

- 9.6 The person may withdraw or vary the undertaking at any time, but only with the written consent of the Information Commissioner.
- 9.7 The Information Commissioner may cancel the undertaking by written notice.
- 9.8 When considering whether to consent to the withdrawal or variation of an undertaking, the Information Commissioner may consider those matters referred to in section 8.9 of these guidelines.

General approach to enforcing undertakings

- 9.9 Under section 33F of the Privacy Act, if the Information Commissioner considers that the entity has breached an undertaking they have given under section 33E, and that undertaking has not been withdrawn or cancelled, the Information Commissioner may apply to the Federal Court or the Federal Circuit Court for one or more of the orders listed in that section:
- a) an order directing the entity to comply with the undertaking;
 - b) any order that the court considers appropriate directing the entity to compensate any other person who has suffered loss or damage as a result of the breach;
 - c) any other order that the court considers appropriate.
- 9.10 When determining whether to seek an order from the Federal Court or the Federal Circuit Court to enforce an undertaking, the Information Commissioner may consider those matters referred to in section 8.11 of these guidelines.

10 Determinations under the Privacy Act

Legislative basis for making a determination

- 10.1 Upon completing the investigation of a complaint made under section 36 of the Privacy Act, the Information Commissioner may, under section 52 of that Act, make a determination that either dismisses the complaint or, if the Information Commissioner has found the complaint to be substantiated, make one or more of the declarations specified in paragraph 52(1)(b) of the Privacy Act.
- 10.2 Upon completing a Commissioner initiated investigation, the Information Commissioner may make a determination that includes one or more of the declarations specified in subsection 52(1A).

Legislative basis for enforcing determination

- 10.3 Under section 55A of the Privacy Act, the Information Commissioner may apply to the Federal Court or the Federal Circuit Court for an order to enforce a determination made under section 52 against a person or entity.

Legislative basis for enforcing determination against an agency

- 10.4 Under section 62 of the Privacy Act, the Information Commissioner may apply to the Federal Court or the Federal Circuit Court for an order to enforce a determination made under section 52 against an agency.
- 10.5 The Information Commissioner may only make an application under section 62 if the agency has failed to comply with its obligations under section 58 of the Privacy Act. Section 58 requires an agency that is the respondent to a section 52 determination to refrain from conduct that has been declared to be an interference with privacy, and to perform any act or course of conduct that was declared, in the determination, to be appropriate to redress any loss or damage.

General approach to making determinations

- 10.6 The Information Commissioner has a discretion, after investigating a complaint made under section 36 of the Privacy Act, to make a determination under subsection 52(1) of the Privacy Act which either dismisses the complaint or finds that the complaint is substantiated.
- 10.7 When investigating a complaint relating to the My Health Record system under the Privacy Act, the Information Commissioner must make a reasonable attempt to conciliate the complaint.
- 10.8 When deciding whether to make a determination under section 52 of the Privacy Act in response to a complaint under section 36, the Information Commissioner may consider:
- a) the particular facts of the matter;
 - b) the factors referred to at section 7.1 of these guidelines;

- c) whether it appears there is a prima facie interference with privacy, the parties are unable to resolve the matter through conciliation and the matter cannot otherwise be finalised;
 - d) whether one or both of the parties has requested that the matter be finalised by way of a determination and the Information Commissioner considers that making a determination would be the appropriate resolution in the particular circumstances;
 - e) whether the issues raised by the complaint are complex and/or systemic
 - f) whether the investigation process has been able to resolve whether an interference with privacy has occurred, and whether it is likely that the determination process would resolve that question.
- 10.9 The Information Commissioner has a discretion, after an investigation on the Commissioner's own initiative, to make a determination under subsection 52(1A) of the Privacy Act.
- 10.10 When deciding whether to make a determination following a Commissioner initiated investigation, the Information Commissioner may consider:
- a) the particular facts of the matter;
 - b) the factors referred to at section 7.1 of these guidelines;
 - c) whether it appears there is a prima facie interference with privacy;
 - d) whether the person has cooperated with the Information Commissioner's enquiries or investigation, and if not, whether the Commissioner believes that it is necessary to make formally binding declarations that the person must take certain steps to address the interference with privacy;
 - e) whether there is a disagreement between the Information Commissioner and the person about whether an interference with privacy has occurred and, if so, the determination would allow that question to be resolved;
 - f) whether there is a public interest in the Information Commissioner making a declaration setting out his or her reasons for finding that an interference with privacy has occurred.

General approach to enforcing determinations

- 10.11 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 the Federal Court or the Federal Circuit Court to enforce the determination.
- 10.12 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;
- c) the Commonwealth's model litigant obligations referred to at section 7.5 of these guidelines.

11 Injunctions under the My Health Records Act

Legislative basis for injunctions

- 11.1 Under section 81 of the My Health Records Act, the Information Commissioner may apply to a Court for an injunction:
- a) seeking an interim order pending final determination of the matter;
 - b) requiring a person to do an act or thing, if the refusal or failure to do that act or thing was, is, or would be a contravention of the My Health Records Act;
 - c) requiring a person to do an act or thing, if the person has engaged, is engaging or is proposing to engage in conduct contravening the My Health Records Act;
 - d) restraining a person from engaging in conduct that constituted, constitutes or would constitute a contravention of the My Health Records Act.
- 11.2 Section 81 of the My Health Records Act triggers the provisions of Part 7 of the Regulatory Powers Act which deals with obtaining, imposing and discharging injunctions to enforce legislative provisions.

General approach to seeking injunctions

- 11.3 In 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;
 - c) the Commonwealth's model litigant obligations referred to at section 7.5.

12 Injunctions under the Privacy Act

- 12.1 Under section 98 of the Privacy Act, the Information Commissioner may apply to the Federal Court or the Federal Circuit Court for an injunction:
- a) seeking an interim order restraining a person from engaging in conduct pending final determination of a matter;
 - b) requiring a person to do an act or thing, if the refusal or failure to do that act or thing was, is, or would be a contravention of the Privacy Act;

- c) requiring the person to do any act or thing if the person has engaged, is engaging or is proposing to engage in conduct contravening the Privacy Act;
 - d) restraining a person from engaging in conduct that constituted, constitutes or would constitute a contravention of the Privacy Act.
- 12.2 In deciding whether to seek an injunction from the Federal Court or the Federal Circuit Court, the Information Commissioner may consider those matters referred to in section 11.3 of these guidelines.

13 Civil penalties under the My Health Records Act

Legislative basis for seeking a civil penalty order

- 13.1 Under section 79 of the My Health Records Act, the Information Commissioner may apply to a Court for an order that a person who is alleged to have contravened a civil penalty provision pay a pecuniary penalty to the Commonwealth. The Information Commissioner must make the application within four years of the alleged contravention.
- 13.2 Section 79 triggers 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.
- 13.3 An overview of the civil penalty provisions in the My Health Records Act is provided below:
- a) sections 59 and 60 – unauthorised collection, use or disclosure, as well as secondary disclosure, of health information in a healthcare recipient’s digital record;
 - b) section 74 – a registered healthcare provider organisation providing insufficient information to identify the individual who requests access to a healthcare recipient’s digital record on behalf of the registered healthcare provider organisation;
 - c) section 75 – failure of an entity which is, or has at any time been, a registered healthcare provider organisation, registered repository operator, registered portal operator or registered contracted service provider to report a data breach in accordance with the requirements of section 75;
 - d) section 76 – failure to notify the System Operator, within the required timeframe, in writing of becoming ineligible to be registered as a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider;

- e) section 77 – the System Operator, a registered repository operator, a registered portal operator or a registered contracted service provider holding, taking, processing or handling My Health Record system records outside Australia, or causing or permitting another person to hold, take, process or handle My Health Record system records outside Australia;
 - f) section 78 – contravention of the My Health Record Rules by a person who is, or has at any time been, a registered healthcare provider organisation, registered repository operator, registered portal operator or registered contracted service provider.
- 13.4 Subsection 82(5) of the Regulatory Powers Act specifies the maximum pecuniary penalty that a Court may impose.

General approach to civil penalties

- 13.5 In deciding whether to seek an order imposing a civil penalty, the Information Commissioner may consider:
- a) the particular facts of the matter;
 - b) the factors referred to at section 7.1 of these guidelines;
 - c) the Commonwealth's model litigant obligations referred to at section 7.5 of these guidelines;
 - d) the guiding principle that the Information Commissioner is unlikely to seek a civil penalty order for minor or inadvertent contraventions, where the person responsible for the contravention has co-operated with the investigation and taken steps to avoid future contraventions.

14 Civil penalties under the Privacy Act

Legislative basis for seeking a civil penalty order

- 14.1 Under section 80W(1) of the Privacy Act, the Information Commissioner may apply to the Federal Court or the Federal Circuit Court for an order that a person who is alleged to have contravened a civil penalty provision of that Act pay a pecuniary penalty to the Commonwealth.
- 14.2 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. Section 13G of the Privacy Act, relating to serious and repeated interferences with privacy, is a civil penalty provision. Therefore, particular conduct may contravene both a civil penalty provision in the My Health Records Act and the 'serious or repeated interference with privacy' civil penalty provision 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.

General approach to civil penalties

- 14.3 In deciding whether to seek a civil penalty order under the Privacy Act, the Information Commissioner may consider the matters referred to in section 13.5 of these guidelines.

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.