

EXPLANATORY STATEMENT

My Health Records Act 2012

My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016

Purpose and authority

The *My Health Records Act 2012* (My Health Records Act) establishes the My Health Record system. The Australian Information Commissioner (the Information Commissioner) has various enforcement and investigative powers in respect of the My Health Record system, under both the My Health Records Act and the *Privacy Act 1988* (Privacy Act).

Section 111 of the My Health Records Act provides for the Information Commissioner to make enforcement guidelines outlining how he or she will approach enforcement issues under the My Health Records Act and related legislation (for example, the Privacy Act) (subsection 111(2)). The Information Commissioner must then have regard to these guidelines in exercising his or her investigative and enforcement powers in relation to the My Health Record system (subsection 111(1)). The purpose of these guidelines is to promote transparency in the Information Commissioner's processes, given the Information Commissioner's important role in relation to the My Health Record system.

Background

The My Health Record system aims to enable the secure sharing of health information between a registered healthcare recipient's registered healthcare provider organisations, while enabling the healthcare recipient to control who can access their My Health Record. A healthcare recipient's My Health Record provides a summary of his or her health information, which is held by the National Repositories Service as well as registered repository operators. Registered repositories may be operated by either private or public sector bodies that must register with the System Operator and comply with any My Health Record Rules that apply to their registration.

The My Health Records Act establishes and regulates the My Health Record system including establishing certain privacy protections. It prescribes the circumstances in which entities can collect, use and disclose health information included in a healthcare recipient's My Health Record. It also allows for the Information Commissioner to seek a range of remedies, including civil penalties, where there is an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record, or where certain actions, events or circumstances occur that might compromise the security or integrity of the My Health Record system.

The Information Commissioner has investigative powers and functions under both the My Health Records Act and the Privacy Act to carry out these enforcement powers and functions. Enforcement powers in the Privacy Act are also available where a matter is investigated under the Privacy Act. This legislative instrument sets out the Commissioner's general approach to the exercise of these investigative and enforcement powers and functions.

The My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 (the guidelines) replace the PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013.

Consultation

Before making the guidelines, the Office of the Australian Information Commissioner (OAIC) took the following steps to consult with stakeholders:

- On 6 October 2015 the OAIC posted on its website a draft of the guidelines together with a summary of the key proposed changes to the guidelines and invited public comment. The period allowed for public consultation was 4 weeks. The closing date for submissions was 3 November 2015.
- The OAIC wrote to various key stakeholders with information about the draft guidelines, providing a summary of the proposed changes to the guidelines and inviting comment. The OAIC also promoted the draft guidelines through other communication channels such as the OAIC's email newsletter, OAICnet, Twitter and a banner on the homepage of the OAIC's website.
- The OAIC received 9 non-confidential submissions as a result of the public consultation. Two of these submitters were granted an extension of time in which to provide a submission and the final submission was received on 13 November 2015.
- The OAIC made some variations to the draft guidelines as a result of the consultation process.

Other issues

This instrument commences on the day after it is registered on the Federal Register of Legislation.

This instrument is a legislative instrument for the purposes of the *Legislation Act 2003*.

An item by item description of this legislative instrument is at the [Attachment](#).

Item-by-item description of the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*

Part 1 Preliminary

Section 1 Name of instrument

Section 1 provides that this instrument is the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (the guidelines).

Section 2 Commencement

Section 2 provides that the guidelines commence on the day after the instrument is registered on the Federal Register of Legislation. It also states that the *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013* are repealed when these guidelines commence.

Section 3 Definitions

This section defines various terms used in the guidelines.

It also clarifies that, unless the contrary intention appears, terms used in the guidelines have the same meaning as in the *My Health Records Act 2012* (My Health Records Act).

Section 4 Introduction

This section briefly explains the My Health Record system and the role of the Information Commissioner and the guidelines in that context.

Sections 4.1 and 4.2 explain that the Information Commissioner is a statutory office holder appointed under subsection 14(1) of the *Australian Information Commissioner Act 2010* (AIC Act), or appointed under section 21(1) of the AIC Act. The Information Commissioner performs functions and exercises powers conferred on the position by the AIC Act and other Acts. Among other things, this includes performing functions and exercising powers in relation to the My Health Record system.

Section 4.3 explains that the My Health Record system is established under and regulated by the My Health Records Act, and that it has the purpose of enabling the secure sharing of a healthcare recipient's health information between his or her registered healthcare provider organisations. The healthcare recipient will have control over who can access his or her health information.

Sections 4.4 and 4.5 explain how the My Health Record system works.

Section 4.6 explains that the My Health Record System Operator is responsible for the operation of the My Health Record system.

Section 4.7 states that the collection, use and disclosure of health information included in a healthcare recipient's My Health Record is regulated by the My Health Records Act and regulations and rules made under that Act.

Sections 4.8 and 4.9 clarify that, in addition to the requirements of the My Health Records Act, participants in the My Health Record system are subject to the *Privacy Act 1988* (the Privacy Act) and relevant State and Territory privacy laws.

Section 4.10 describes the functions of Information Commissioner in relation to the My Health Record system. The Information Commissioner has the role of investigating alleged contraventions of the My Health Records Act and addressing such contraventions as appropriate through conciliation, education and enforcement action.

Section 4.11 sets out the range of avenues by which an alleged contravention of the My Health Records Act may be brought to the Information Commissioner's attention.

Sections 4.12 to 4.14 describe the role of the guidelines. These sections explain that the guidelines are made under section 111 of the My Health Records Act and set out the Information Commissioner's general approach to the exercise of his or her investigative and enforcement powers in relation to the My Health Record system. Section 4.14 makes it clear that, despite the general approach provided in the guidelines, the Information Commissioner maintains discretion to exercise the available powers that he or she considers the most appropriate in the 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

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

This section sets out the types of enforcement and investigative powers that the Information Commissioner has in relation to the My Health Record system.

Section 5.1 explains that there are relevant enforcement and investigative powers available to the Information Commissioner under both the My Health Records Act and the Privacy Act. These powers are based on an escalation model.

Section 5.2 describes the Information Commissioner's investigative powers under the My Health Records Act. This provision empowers the Information Commissioner 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. The alleged contravention must be either in connection with a healthcare recipient's health information, or a breach of a civil penalty provision.

Sections 5.3 to 5.5 describe the Information Commissioner's investigative powers under the Privacy Act. Section 5.3 explains that, given that a contravention of the My Health Records Act involving health information included in a My Health Record or a provision of Part 4 or 5 is an interference with privacy, the Information Commissioner may investigate that act or practice under the Privacy Act. Part 4 of the My Health Records Act deals with the collection, use and disclosure of health information included in a healthcare recipient's My Health Record. Part 5 of the My Health Records Act outlines a series of civil penalty provisions.

Section 5.4 states that Part V of the Privacy Act sets out the relevant investigative powers and processes that would apply when the Information Commissioner conducts an investigation under the Privacy Act into an alleged contravention of the My Health Records Act.

Section 5.5 lists a range of investigative powers available to the Information Commissioner under Part V of the Privacy Act. This section further notes that Part V of the Privacy Act also sets out procedural requirements for an investigation.

Sections 5.6 and 5.7 describe the enforcement powers that are available to the Information Commissioner under the My Health Records Act. These include the ability to accept an enforceable undertaking, and to apply to a Court for an order to enforce an undertaking, for an injunction or for a civil penalty order.

Sections 5.8 and 5.9 describe the enforcement powers that are available to the Information Commissioner under the Privacy Act. These include the power to accept an enforceable undertaking and to make a non-binding determination. The Information Commissioner may apply to the Federal

Court or the Federal Circuit Court for an order to enforce an enforceable undertaking or a determination, to seek an injunction or for a civil penalty order.

Section 6 Investigations – general principles

This section sets out the general principles that the Information Commissioner will apply when investigating an alleged contravention.

Section 6.1 explains that the Information Commissioner will act consistently with general principles of good decision making, as outlined in the *Best Practice Guides* published by the Administrative Review Council. In particular, the Information Commissioner will act fairly, transparently, and in accordance with principles of natural justice (or procedural fairness).

Sections 6.2 and 6.3 set out the Information Commissioner's general approach to complaints relating to the My Health Record system. A complaint will generally be treated as a complaint made under section 36 of the Privacy Act, unless there is a reason to accept the complaint and act under the My Health Records Act. Section 6.3 explains that, when investigating a complaint relating to the My Health Records system under the Privacy Act, the Information Commissioner must make a reasonable attempt to conciliate the complaint. Following a complaint investigation, enforcement action may be taken under either the Privacy Act or the My Health Records Act.

Sections 6.4 to 6.6 describe the Information Commissioner's approach to Commissioner initiated investigations, which may be undertaken following a complaint or data breach notification or independently of any complaint or notification. Such investigations will be conducted under Part V of the Privacy Act, unless there is a reason to conduct the investigation under the My Health Records Act. Following an investigation, enforcement action may be taken under either the Privacy Act or the My Health Records Act.

Sections 6.7 and 6.8 set out the Information Commissioner's general approach to conducting investigations under section 73 of the My Health Records Act. Section 6.7 states that the process will follow, as far as practicable, the processes established in Part V of the Privacy Act. Section 6.8 states that, following an investigation under section 73, the Information Commissioner may take enforcement action under the My Health Records Act

Section 7 Enforcement action – general principles

Section 7.1 outlines the 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. Examples include the seriousness of the incident and the likelihood that the individual or entity will contravene the My Health Records Act or Privacy Act in future. Section 7.2 states that the Information Commissioner can use a combination of enforcement powers to address a particular contravention.

Sections 7.3 and 7.4 explain the Information Commissioner's powers to disclose information or documents to the My Health Record System Operator that relate to an investigation being conducted in relation to the My Health Record system. Section 7.3 states that the My Health Records Act authorises the Information Commissioner to disclose to the My Health Record System Operator any information or documents that relate to an investigation if the Commissioner is satisfied that doing so will enable the My Health Record System Operator to monitor or improve the operation or security of the My Health Records Act. Section 7.4 explains that a disclosure under section 73A of the My Health Records Act may also assist the My Health Record System Operator in exercising the power to cancel, suspend or vary a person's My Health Record registration.

Section 7.5 outlines the general litigation principle that the Information Commissioner act in accordance with the *Commonwealth's Legal Services Directions 2005*.

Sections 7.6 to 7.8 discuss the Information Commissioner's publication of his or her use of enforcement powers. They explain that the Information Commissioner may communicate publicly about the use of enforcement powers, and will generally publish enforceable undertakings accepted under either the Privacy Act or My Health Records Act, and determinations made under section 52 of the Privacy Act.

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

Part 3 of the guidelines explains, in more detail, the range of enforcement mechanisms available to the Information Commissioner under the My Health Records Act and the Privacy Act.

Section 8 Enforceable undertakings under the My Health Records Act

Section 8.1 explains that section 80 of the My Health Records Act allows the Information Commissioner to accept a written undertaking that a person will, in order to comply with the My Health Records Act, either take or refrain from taking specified action, or that the person will take specified action directed to ensuring future compliance with the My Health Records Act.

Section 8.2 explains that section 80 of the My Health Records Act triggers the provisions of Part 6 of the *Regulatory Powers Act (Standard Provisions) Act 2014* (Regulatory Powers Act). Part 6 of the Regulatory Powers Act deals with the acceptance and enforcement of undertakings relating to compliance with legislative provisions.

Section 8.3 provides that the individual giving and executing the undertaking must have the authority to negotiate on behalf of, and bind, the respondent.

Sections 8.4 and 8.5 relate to the terms of an enforceable undertaking – what the terms should include and what terms are considered unacceptable by the Information Commissioner.

Section 8.6 explains the factors that the Information Commissioner may take into account when deciding whether to accept an undertaking in a particular matter.

Sections 8.7 to 8.9 relate to the withdrawal, variation or cancellation of an undertaking. Section 8.7 explains that a person may withdraw or vary an undertaking only with the written consent of the Information Commissioner. Section 8.8 states that the Information Commissioner can cancel an undertaking by written notice. Section 8.9 lists the circumstances that generally must exist before the Information Commissioner would consent to the variation or withdrawal of an undertaking, such as compliance with the undertaking being subsequently found to be impractical.

Sections 8.10 and 8.11 outline the general approach to enforcing undertakings, including the types of orders that the Information Commissioner can apply to a Court for, and the factors the Information Commissioner may take into account when deciding whether to seek an order from a Court to enforce an undertaking.

Section 9 Enforceable undertakings under the Privacy Act

Section 9.1 explains that under section 33E of the Privacy Act, the Information Commissioner may accept a written undertaking given by an entity that an entity will refrain from or take specified action to comply with the Privacy Act, or take specific action to ensure the entity does not interfere with the privacy of an individual.

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

Section 9.3 states that the terms in section 8.4 of these guidelines should be included in any undertaking to be accepted by the Information Commissioner.

Section 9.4 explains that the Information Commissioner will not accept an enforceable undertaking under the Privacy Act if it includes any terms in section 8.5 of these guidelines.

Section 9.5 explains that the Information Commissioner may consider the matters referred to in section 8.6 of these guidelines when deciding whether to accept an undertaking under the Privacy Act.

Sections 9.6 to 9.8 outline the conditions for withdrawing, varying and cancelling an undertaking that is accepted by the Information Commissioner.

Sections 9.9 and 9.10 outline the general approach to enforcing undertakings. Section 9.9 explains that under section 33F of the Privacy Act, if the Information Commissioner considers that the entity has breached an undertaking that 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 section 33F of the Privacy Act. Section 9.10 states that the Information Commissioner may consider the matters referred to in section 8.11 of these guidelines when determining whether to seek a Court order to enforce an undertaking.

Section 10 Determinations under the Privacy Act

Section 10.1 explains that the Information Commissioner may, upon completing the investigation of a complaint made under section 36 of the Privacy Act, make a determination under section 52 of that Act that either dismisses the complaint or finds it to be substantiated.

Section 10.2 explains that the Information Commissioner, upon completing a Commissioner initiated investigation, may make a determination that includes one or more of the declarations specified in subsection 52(1A) of the Privacy Act.

Section 10.3 explains that section 55A of the Privacy Act allows the Information Commissioner to apply to the Federal Court or the Federal Circuit Court to enforce a determination against a person or entity.

Section 10.4 explains that section 62 of the Privacy Act allows the Information Commissioner to apply to the Federal Court or the Federal Circuit Court to enforce a determination against an agency.

Section 10.5 clarifies that 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. These obligations include refraining from conduct that has been declared to be an interference with privacy, and to perform any act or conduct that was declared in the section 52 determination to be appropriate redress.

Sections 10.6 to 10.10 set out the Information Commissioner's general approach in relation to making determinations under section 52 of the Privacy Act.

Section 10.6 clarifies that the Information Commissioner has a discretion, after investigation a complaint under section 36 of the Privacy Act, to make a determination which either dismisses the complaint or finds it substantiated.

Section 10.7 states that the Information Commissioner must make a reasonable attempt to conciliate complaints relating to the My Health Record system.

Section 10.8 lists the factors which the Information Commissioner may consider when deciding whether to make a determination under section 52 of the Privacy Act in response to a complaint.

Section 10.9 states that the Information Commissioner has a discretion to make a determination under subsection 52(1A) of the Privacy Act, after an investigation on the Commissioner's own initiative.

Section 10.10 lists the factors that the Information Commissioner may consider when deciding whether to make a determination following a Commissioner initiated investigation.

Section 10.11 states that 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 Court to enforce the determination.

Section 10.12 lists the factors that the Information Commissioner may consider when deciding whether to commence proceedings to enforce a determination.

Section 11 Injunctions under the My Health Records Act

Section 11.1 explains that section 81 of the My Health Records Act allows the Information Commissioner to apply to a Court for an injunction that requires a person to do an act or thing, or that restrains a person from doing an act or thing, in order to prevent a contravention of the My Health Records Act.

Section 11.2 states that 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.

Section 11.3 lists the factors that the Information Commissioner may consider in deciding whether to seek an injunction from a Court.

Section 12 Injunctions under the Privacy Act

Section 12.1 explains that section 98 of the Privacy Act allows the Information Commissioner to apply to a Court for an injunction that requires a person to do an act or thing, or that restrains a person from doing an act or thing, in order to prevent a contravention of the Privacy Act.

Section 12.2 states that the Information Commissioner may consider the matters referred to in section 11.3 of these guidelines in deciding whether to seek an injunction from the Court.

Section 13 Civil penalties under the My Health Records Act

Section 13.1 states that under section 79 of the My Health Records Act, the Information Commissioner may apply to a Court for an order that a person who has contravened a civil penalty provision pay a pecuniary penalty to the Commonwealth.

Section 13.2 states that section 79 of the My Health Records Act 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.

Section 13.3 provides an overview of the civil penalty provisions in the My Health Records Act.

Section 13.4 states that the maximum pecuniary penalty that a Court may impose is specified in subsection 82(5) of the Regulatory Powers Act.

Section 13.5 outlines the considerations the Information Commissioner may take into account in deciding whether to seek an order imposing a civil penalty. In particular, the section notes that the Information Commissioner is unlikely to seek a civil penalty order for a minor or inadvertent

contravention or where the person has co-operated with the investigation and taken steps to avoid future contraventions.

Section 14 Civil penalties under the Privacy Act

Sections 14.1 and 14.2 outline the legislative basis for seeking a civil penalty order under the Privacy Act for contraventions of the My Health Record system. Section 14.1 states that the Information Commissioner can apply to a Court for an order that a person pay a pecuniary penalty under section 80W(1) of the Privacy Act.

Section 14.2 explains that a contravention of the My Health Records Act in connection with health information included in a healthcare recipient's My Health Record or a contravention of a provision of Part 4 or 5 is an interference with privacy for the purposes of the Privacy Act. Particular conduct may contravene both a civil penalty provision in the My Health Records Act and a civil penalty provision in the Privacy Act.

Section 14.3 states that the Information Commissioner may consider the matters referred to in Section 13.5 of these guidelines in deciding whether to seek a civil penalty order under the Privacy Act from the Court.

Statement of Compatibility with Human Rights - prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016

This legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of legislative instrument

This legislative instrument is made under section 111 of the *My Health Records Act 2012* (the My Health Records Act). It describes the Information Commissioner's investigative and enforcement powers under both the My Health Records Act and the *Privacy Act 1988* (Privacy Act) and sets out the Information Commissioner's general approach to the exercise of these powers in relation to the My Health Record system.

Human rights implications

The legislative instrument engages the following human rights:

Right to protection of privacy and reputation

Article 17 of the International Covenant on Civil and Political Rights guarantees protection from, among other things, arbitrary or unlawful interference with a person's privacy.

This legislative instrument engages with Article 17 by supporting the enforcement and compliance aspects of the My Health Record system, which include a specific privacy regime for the handling of a registered healthcare recipient's health information which will generally operate concurrently with Commonwealth, state and territory privacy laws.

In particular, this legislative instrument sets out the Information Commissioner's general approach when using the available investigatory and enforcement powers. It makes it clear that the Information Commissioner will investigate unlawful interferences with privacy consistently, whether under the Privacy Act or the My Health Records Act. The Information Commissioner will, where appropriate, pursue available enforcement mechanisms against persons who have contravened privacy laws in relation to the My Health Record system.

Right to enjoyment of highest attainable standard of health

This legislative instrument also engages Articles 2 and 12 of the International Covenant on Economic, Social and Cultural Rights by assisting with the progressive realisation by all appropriate means of the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.

This legislative instrument supports the administration of the My Health Record system, the intention of which is to enable a safer, higher quality, more equitable and sustainable health system for all Australians by transforming the way information is used to plan, manage and deliver healthcare services. The My Health Record system arose out of the National E-Health Strategy and National Health and Hospitals Reform Commission report of June 2009, which both identified an electronic health records system as being central to enabling the realisation of many health reform objectives including improved quality, safety, efficiency and equity in healthcare and the long-term sustainability of the health system.

Conclusion

The legislative instrument is compatible with human rights because it advances the protection of human rights.

Timothy Pilgrim, Acting Australian Information Commissioner