Chapter 3: Enforceable undertakings

Contents

Legislative framework

3.1 An enforceable undertaking is a written agreement between an entity or person (the respondent) and the Commissioner, which is provided under either the Privacy Act, the My Health Records Act or the Competition and Consumer Act, and is enforceable against the respondent in the courts.

Enforceable undertaking under the Privacy Act

3.2 Section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) empowers the Commissioner to accept a written undertaking given by an entity that it will either:

- take specified action in order to comply with the Privacy Act
- refrain from taking specified action in order to comply with the Privacy Act
- take specified action directed towards ensuring that the entity does not contravene a provision under the Privacy Act, or is unlikely to contravene such a provision in the future.

3.3 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner (s 114 (3) of the Regulatory Powers Act), or cancelled by the Commissioner (s 114 (5) of the Regulatory Powers Act).

3.4 If the Commissioner considers that an entity has breached an undertaking, the Commissioner may apply to the Federal Court or Federal Circuit Court to enforce the undertaking (ss 113 and 115 of the Regulatory Powers Act, s 80V of the Privacy Act).

Enforceable undertaking under the My Health Records Act

3.5 Under s 114 of the Regulatory Powers Act, the Commissioner may accept a written undertaking in relation to the My Health Records Act given by a person that the person will:

- take specified action in order to comply with the My Health Records Act
- refrain from taking specified action, in order to comply with the My Health Records Act
- 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.

3.6 Section 80 of the My Health Records Act triggers the provisions of Part 6 of the Regulatory Powers Act which provides a framework for accepting and enforcing undertakings relating to compliance with legislative provisions. This means that the Commissioner may accept an undertaking relating to compliance with a My Health Records Act provision that is enforceable under Part 6 of the Regulatory Powers Act.

3.7 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner, or cancelled by the Commissioner.

3.8 If the Commissioner considers that a person has breached an undertaking accepted under s 80 of the My Health Records Act and that undertaking has not been withdrawn or cancelled, the Information Commissioner may apply to the relevant court for an order directing the person to comply with the undertaking (or one or more of the orders listed in Part 6 of the Regulatory Powers Act).

Enforceable undertaking under the Competition and Consumer Act

3.9 Under s 114 of the Regulatory Powers Act, the Commissioner may accept a written undertaking in relation to the CDR scheme as set out in the Competition and Consumer Act, given that the person will:

- take specified action in order to comply with the privacy safeguards
- refrain from taking specified action, in order to comply with the privacy safeguards

- take specified action directed towards ensuring that the person does not contravene the privacy safeguards, or is unlikely to contravene the privacy safeguards, in the future.

3.10 Section 56EW of the Competition and Consumer Act triggers the provisions of Part 6 of the Regulatory Powers Act which provides a framework for accepting and enforcing undertakings relating to compliance with legislative provisions. This means that the Commissioner may accept an undertaking relating to compliance with a privacy safeguard provision that is enforceable under Part 6 of the Regulatory Powers Act.

3.11 An enforceable undertaking may be varied or withdrawn with the consent of the Commissioner, or cancelled by the Commissioner.

3.12 If the Commissioner considers that a person has breached an undertaking accepted under s 56EW of the Competition and Consumer Act and that undertaking has not been withdrawn or cancelled, the Commissioner may apply to the relevant court for an order directing the person to comply with the undertaking (or one or more of the orders listed in Part 6 of the Regulatory Powers Act).

Which Act to use?

3.13 Acts or practices that interfere with an individual's privacy but do not relate to a contravention of the My Health Records Act, or to a privacy safeguard set out in Part IVD of the Competition and Consumer Act, are governed by the Privacy Act and an enforceable undertaking that relates to those acts or practices will be accepted by the Commissioner under the Privacy Act.

3.14 Acts or practices that contravene certain provisions of the My Health Records Act are deemed by s 73 of that Act to be an interference with an individual's privacy for the purposes of the Privacy Act. Depending on the circumstances, an enforceable undertaking in relation to these contraventions may be able to be accepted under the My Health Records Act or the Privacy Act.

3.15 Sub-section 80(2) of the My Health Records Act also empowers the My Health Record System Operator[1] to accept enforceable undertakings. The Commissioner may consult with the System Operator when investigating a complaint and considering accepting an undertaking, in line with the *Agreement for information sharing and complaint referral relating to the personally controlled electronic health (eHealth) record system between the OAIC and the System Operator*.[2]

3.16 For conduct that is a breach of a privacy safeguard, the Commissioner may accept an enforceable undertaking under the Competition and Consumer Act.

[1] 'System Operator' is defined in s 14 of the My Health Records Act.

[2] The agreement can be viewed on the OAIC's website.

Purpose and key features of an enforceable undertaking

3.17 An enforceable undertaking is an important enforcement tool for use in situations where there has been or appears to have been an interference with the privacy of an individual[3] and the Commissioner considers an agreed change to future behaviour offers the most appropriate regulatory outcome in the particular circumstances.

3.18 Generally, an enforceable undertaking seeks to have a respondent voluntarily agree to:

- modify its acts, practices, procedures or behaviour to ensure it complies with the law (for example, ceasing the practice that led to the breach or implementing new policies for handling personal information)
- remedy the damage any breach has caused (for example making an apology or making a payment to an individual or individuals to rectify damage)
- commit to certain future compliance measures (for example conducting reviews and audits, providing training for managers and staff and implementing a compliance monitoring and reporting framework).

Who can give an enforceable undertaking?

3.19 An enforceable undertaking for conduct under the Privacy Act can only be given by 'an entity'. The term 'entity' means an agency, an organisation or a small business operator (these terms are further defined in s 6(1) of the Privacy Act). The term 'organisation' can include an individual (including a sole trader).

3.20 An enforceable undertaking for conduct under the My Health Records Act and the Competition and Consumer Act can be given by 'a person'.[4] This term captures both individuals and participants in the My Health Record system, such as registered repository operators, portal operators and healthcare provider organisations.

3.21 For each undertaking, the individual giving and executing the undertaking must have the authority to negotiate on behalf of, and bind, the respondent entity or person.

At what point can an enforceable undertaking be accepted?

3.22 The Commissioner may accept an enforceable undertaking given by an entity or person where the Commissioner considers there is a reasonable basis to suggest that the entity or person has interfered with the privacy of an individual. For example, an enforceable undertaking may be accepted during a complaint investigation, an enquiry into a data breach incident, or a Commissioner initiated investigation.

---

[3] The *Privacy regulatory action policy* and the My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 outline the range of avenues through which the OAIC may become aware of alleged interferences with privacy or other privacy concerns.

[4] The term 'person' is not defined in the My Health Records Act and the Competition and Consumer Act, so the meaning is drawn from the *Acts Interpretation Act 1901* (Cth). That Act states that expressions used to denote persons generally, such as 'person', include a body politic or body corporate as well as an individual (s 2C).

3.23 An enforceable undertaking may form part of a conciliated outcome following a complaint. Section 40A of the Privacy Act requires the Commissioner to make a reasonable attempt to conciliate a complaint where the Commissioner considers there is a reasonable possibility that the complaint can be conciliated successfully.

Enforceable undertaking terms and requirements

3.24 The Privacy Act, the My Health Records Act and Part IVD of the Competition and Consumer 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.

3.25 In addition, the OAIC expects that the terms of any undertaking will usually (at a minimum):

- state the name of the respondent, the date the undertaking was accepted by the Commissioner and the date when the undertaking comes into effect
- be signed by the CEO or other senior executive of the respondent and the Commissioner (or approved delegate) – without the signature of both parties, the undertaking has no effect
- describe and acknowledge the act(s) or practice(s) about which the OAIC is concerned
- outline specified steps the respondent will take to rectify the act or practice, and ensure that it is not repeated or continued. This will usually include a requirement for the respondent to complete reviews and establish a monitoring and reporting framework. Specifically, the respondent will usually be required to:
    - nominate in writing a representative responsible for overseeing compliance with the undertaking and reporting to the OAIC
    - engage, in consultation with the OAIC, an appropriately experienced and qualified third party to review the act or practice and make recommendations to improve the respondent's compliance with the Privacy Act (the Independent Expert)
    - ensure that the OAIC receives a copy of the Independent Expert's report, including a copy of the Independent Expert's draft report prior to engagement with the respondent
    - implement the recommendations in that report
    - provide a certification by the Independent Expert to the OAIC that the respondent has implemented the recommendations and rectified the deficiencies identified by the review
- outline what, if any, steps the respondent will take to notify individuals affected by the act or practice, where it has not already done so
- contain dates by which the respondent must complete each step
- be readily understood; for example, an undertaking that deals with complex and technical issues may have a glossary to define the terms used
- be capable of implementation and include action which is capable of being measured or tested objectively
- be certain and capable of enforcement; for example, each step that the respondent is required to complete must be clear and unambiguous

- contain the respondent's agreement to material that arose in conciliation (if conciliation occurred) being submitted in any proceeding to enforce the undertaking.[5] Where an undertaking forms parts of a conciliated outcome, this could be achieved by a statement of agreed facts being attached to the undertaking with the consent of both the respondent and complainant
- outline what, if any, steps the respondent will take to resolve the matter with individuals affected by the act or practice; for example, payment the respondent will make by way of compensation for any loss or damage suffered by reason of the act or practice of concern
- contain the respondent's acknowledgement that the OAIC may publish the undertaking in full (see 'Publication' below for further information). Any concerns the respondent has about publication should be raised and resolved as the terms of the undertaking are being negotiated.

3.26 For undertakings relating to the My Health Record system, reference should also be made to ss 8 and 9 of the My Health Records Enforcement Guidelines when considering the terms of an undertaking.

3.27 The Commissioner will not accept an undertaking that:

- denies responsibility for the act or practice of concern[6]
- merely undertakes to comply with the law without explaining how compliance will be achieved
- seeks to impose terms or conditions on the OAIC or Commissioner (however, the undertaking may include an acknowledgement that certain information provided to the OAIC pursuant to the undertaking is communicated in confidence).

Procedural steps

3.28 When the acceptance of an enforceable undertaking is a possible regulatory outcome in a matter, the OAIC will generally follow the process set out below.

Raising the possibility of an enforceable undertaking

3.29 The possibility of an enforceable undertaking may arise where either:

- the respondent suggests to the OAIC that it gives an undertaking in relation to a matter
- the OAIC raises the possibility of an undertaking with the respondent as a potential option in relation to a matter.

3.30 Before the OAIC raises the possibility of an undertaking, or when the respondent suggests giving an undertaking, the OAIC must assess whether an undertaking offers an appropriate

[5] This is necessary because s 40A(5) of the Privacy Act limits the circumstances in which evidence of anything said or done in the course of the conciliation can be relied upon in legal proceedings. Such material can be used for this purpose where both the respondent and complainant agree. The OAIC would also need to obtain the complainant's agreement before material from a conciliation can be used in enforcement proceedings.

[6] This does not preclude the possibility of an enforceable undertaking being accepted on a 'without prejudice' basis in circumstances where the OAIC considers that it would provide an effective regulatory outcome.

regulatory outcome in a matter, or whether an alternative regulatory outcome would be more appropriate. In making this assessment, the OAIC will refer to the factors set out in the *Privacy regulatory action policy*, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines as applicable.

Negotiating the terms of the enforceable undertaking

3.31 Where the Commissioner considers that an undertaking may be an appropriate regulatory outcome in the matter and the respondent will consider giving an undertaking in relation to the matter, the OAIC and respondent can commence negotiation of the terms of that undertaking.

3.32 When negotiating the terms of the enforceable undertaking, the Commissioner (through the OAIC) will have regard to:

- the requirements for the terms of an undertaking set out above in this chapter or, if the undertaking is related to the My Health Records Act, ss 8.4 and 8.5 and ss 9.3 and 9.4 of the My Health Records Enforcement Guidelines
- the interests of individuals who have been the subject of an interference with privacy
- the OAIC's goal of taking enforcement action and how an undertaking will contribute to fulfilling the OAIC's regulatory role in the particular matter (see the *Privacy regulatory action policy* and *CDR regulatory action policy*)
- the principles guiding regulatory decisions and action outlined in the *Privacy regulatory action policy* or the *CDR regulatory action policy* if applicable, or if the undertaking is related to the My Health Records Act, the My Health Records Enforcement Guidelines.

3.33 Until an undertaking is accepted and signed by the Commissioner, the Commissioner retains the discretion to accept or not accept the undertaking when it is submitted for final approval. Any agreement on terms between OAIC staff and the respondent is 'in principle' agreement only and subject to final acceptance by the Commissioner.

3.34 At the outset of negotiations, the OAIC will identify a reasonable time frame within which any undertaking should be negotiated. If an agreed undertaking cannot be negotiated within that time, the OAIC will consider pursuing alternative enforcement mechanisms such as potential for the Commissioner to make a determination in respect of the matter.

Commissioner considers whether to accept the enforceable undertaking

3.35 Where OAIC staff and the respondent have agreed on terms, the proposed undertaking to be given by the respondent will be submitted to the Commissioner for consideration.

3.36 The decision to accept an undertaking in the terms given by the respondent will be made by the Commissioner.

3.37 Whether the Commissioner accepts an undertaking will be determined on a case by case basis, with reference to the *Privacy regulatory action policy*, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines (as applicable), and whether the Commissioner believes that the respondent has the ability to, and genuinely intends to, comply with the terms of the undertaking.

Approval of the Independent Expert

3.38 The Independent Expert is expected to provide assurance to the Commissioner that the steps planned or taken by the respondent satisfy the terms of the undertaking. The Independent Expert must be competent to undertake the role and independent from the respondent, such that he or she can bring objective and impartial judgment to the role. It is important that the Independent Expert is, and is seen to be, independent.

3.39 It is the responsibility of the respondent and the proposed Independent Expert to demonstrate competence and independence. The Commissioner may make any inquiries considered necessary in order to be satisfied that the proposed Independent Expert brings the requisite competence and independence to the role.

3.40 Factors the Commissioner may consider when determining whether a proposed Independent Expert is competent to undertake the role:

- the qualifications, experience and technical expertise of the proposed Independent Expert, or the senior staff within the relevant entity who will be engaged in the work
- whether the Independent Expert has adequate resources to perform the necessary work
- where appropriate, references from entities regarding the proposed Independent Expert's demonstrated experience in related work.

3.41 Factors the Commissioner may consider when determining whether a proposed Independent Expert is sufficiently independent to undertake the role:

- whether the fees and remuneration received by the proposed Independent Expert from the respondent in the previous two years are material (materiality should be considered in the context of the Independent Expert's Australian-based revenue)
- what other work senior staff proposed to conduct the work of the Independent Expert, have been engaged in for or on behalf of the respondent in the previous two years
- whether there are any staff from the Independent Expert's entity embedded in the respondent's organisation, or otherwise operating under a co-sourcing arrangement
- whether the senior staff proposed to conduct the work of the Independent Expert have ever previously worked for the respondent
- whether the senior staff proposed to conduct the work of the Independent Expert have a financial or other interest in the respondent's business, such as shares
- whether the senior staff proposed to conduct the work of the Independent Expert have previously audited, reviewed, planned, advised or implemented any systems and processes of the respondent, and if so, whether there is a nexus between those systems and processes and the undertaking
- any joint ventures between the proposed Independent Expert and the respondent
- whether the Independent Expert has satisfactory policies and processes in place to ensure that any conflict of interest that arises during the course of the undertaking is managed appropriately and reported to the Commissioner.

Decision communicated to the respondent

3.42 The OAIC will communicate the Commissioner's decision in writing to the respondent.

3.43 Where the Commissioner has agreed to accept the undertaking, this written correspondence will request the respondent to arrange signing of the undertaking by the CEO or other senior executive of the respondent, before returning the signed copy to the OAIC for execution by the Commissioner.

3.44 Where the Commissioner has not agreed to accept the undertaking, the written correspondence will advise the respondent of the OAIC's next steps in the matter. This may involve further negotiations in relation to the proposed undertaking, or consideration of alternative enforcement action.

Undertaking published

3.45 Once the undertaking has been executed by both the respondent and the Commissioner, the OAIC will generally publish the undertaking (see the 'Publication' heading below).

Ongoing monitoring

3.46 It is the respondent's responsibility to ensure it complies with the terms of the undertaking. The OAIC will maintain contact with the respondent and monitor the respondent's compliance, including by ensuring that required reports and notifications are provided in accordance with the timeframes outlined in the enforceable undertaking. If the respondent breaches the undertaking, the OAIC may take further action (see below).

Varying, withdrawing and cancelling an enforceable undertaking

3.47 A respondent can vary or withdraw an enforceable undertaking, but must have the consent of the Commissioner in order to do so.[7]

3.48 The decision as to whether or not to allow a respondent to vary or withdraw an undertaking will be made by the Commissioner on a case-by-case basis.

3.49 The Commissioner generally will only consent to the variation or withdrawal of an undertaking if:

- compliance with the enforceable undertaking is subsequently found to be impractical, or
- there has been a material change in the circumstances which led to the undertaking being given, meaning that variation or withdrawal are appropriate in the circumstances.

3.50 In addition, the Commissioner will only consent to variation or withdrawal where satisfied that an appropriate regulatory outcome will still be achieved in the circumstances. In the case of the withdrawal of an undertaking, the OAIC may decide to take alternative enforcement action.

3.51 A respondent wishing to seek consent to varying or withdrawing an undertaking should make a request in writing to the OAIC. Where the Commissioner consents to the variation or

[7] Privacy Act s 80V, My Health Records Act s80, which trigger Part 6 of the Regulatory Powers Act.

withdrawal of an undertaking, the OAIC will communicate this decision to the respondent in writing.[8]

3.52 In addition, the Commissioner may, by written notice given to the respondent, cancel an undertaking accepted under either the Privacy Act, the My Health Records Act or the Competition and Consumer Act.[9] A decision to cancel an undertaking would normally only be made where subsequent information or conduct by the respondent leads the OAIC to consider that the undertaking is not an effective regulatory outcome in the circumstances. This is only expected to occur in exceptional circumstances, for example, if the Commissioner was misled about the extent of a particular breach.

Breach of an enforceable undertaking

3.53 Where the OAIC believes that a respondent has breached the terms of an enforceable undertaking, the OAIC will generally use the following procedure.

3.54 The OAIC will first bring the issue of suspected or actual non-compliance with the terms of the undertaking to the attention of the respondent and seek a response. This notification and response may be sufficient to resolve the breach.

3.55 The OAIC may decide to address non-compliance through the court enforcement mechanisms in Part 6 of the Regulatory Powers Act. This process is outlined below.

3.56 The factors which the Commissioner will take into account when deciding whether to seek an order from a court to enforce an undertaking are set out in the *Privacy regulatory action policy* and, where applicable, the *CDR regulatory action policy* or the My Health Records Enforcement Guidelines. In addition, the Commissioner will also consider the following factors:

- the nature and length of non-compliance
- the reason for non-compliance
- whether the non-compliance was inadvertent
- whether the respondent had previously not complied with the terms.

3.57 In limited circumstances, the OAIC may initiate further negotiations with the respondent to expand or otherwise vary the terms of the undertaking.

3.58 For an undertaking relating to compliance with the My Health Records Act, the OAIC may also refer the issue to the My Health Record System Operator who has the power to take administrative action against the respondent.

Enforcement through the Court

3.59 Where the OAIC decides to address non-compliance through the court enforcement mechanisms in Part 6 of the Regulatory Powers Act, the Commissioner may apply to a relevant court for one of a number of orders.

---

[8] See s 114(3) of the Regulatory Powers Act.

[9] See s 80V of the Privacy Act, s 80 of the My Health Records Act and s 56EW of the Competition and Consumer Act, which trigger Part 6 of the Regulatory Powers Act; also see s 8.8 of the My Health Records Enforcement Guidelines.

3.60 In general terms, a court may make any or all of the following orders:

- directing the respondent to comply with the undertaking
- directing the respondent to pay compensation
- any other kind that the court thinks appropriate.

Publication

3.61 The OAIC may publish an enforceable undertaking on the OAIC's website (s 80V (4) of the Privacy Act and s 80 (4) of the My Health Records Act).

3.62 Generally, the OAIC will publish an undertaking on its website <www.oaic.gov.au>. An undertaking will usually contain an acknowledgement from the respondent that the undertaking may be published, unless the OAIC has agreed otherwise with the respondent when the undertaking terms were being negotiated (see above). The OAIC may agree otherwise where it is inappropriate to publish all or part of an undertaking because of statutory secrecy provisions or for reasons of privacy, confidentiality, commercial sensitivity, security or privilege.

3.63 The publication of an undertaking may be accompanied by other communications such as a media release, media interview or social media posts. The OAIC generally will also publicly communicate:

- a decision by the Commissioner to vary, withdraw or cancel a published undertaking
- the initiation of court proceedings to enforce an undertaking.

3.64 In addition, before court proceedings are initiated, the OAIC may publicly communicate the fact that a respondent has breached the terms of an undertaking and that the OAIC is making inquiries with the respondent.