General Practice Clinics

APP 1 Privacy Policy assessment

Privacy assessment report
Australian Privacy Principles assessment
Section 33C Privacy Act 1988

Assessments undertaken: May 2015 to June 2015
Final report issued: April 2016
# Contents

Part 1 — Introduction .................................................................................................................................................................................. 1
   Objective and scope of the assessment ............................................................................................................................... 1
   Information required ........................................................................................................................................................................... 1
   Conduct of the assessment ................................................................................................................................................................. 2
   Assessment technique ........................................................................................................................................................................ 2
   Summary statistics and privacy risks ................................................................................................................................. 2
   Resources ................................................................................................................................................................................................ 2

Part 2 — Summary statistics regarding findings ............................................................................................................................... 3

Part 3 — Detailed commentary ........................................................................................................................................................................ 5
   APP 1.5 — Availability and accessibility........................................................................................................................................... 5
   APP 1.3 — Readability and currency ........................................................................................................................................... 6
   APP 1.4 — Contactability ...................................................................................................................................................................... 7
   APP 1.4 — Content: Collection, holding, use and disclosure of personal information ............................................................. 8
   APP 1.4 — Content: Accessing and seeking correction of personal information and making complaints .................................................................................. 10
   APP 1.4 — Content: eHealth .............................................................................................................................................................. 11

Appendix A — Risk based assessments — privacy risk guidance ........................................................................................................... 13

Appendix B — Resources .............................................................................................................................................................................. 14
Part 1 — Introduction

1.1 This report outlines the findings of an assessment by the Office of the Australian Information Commissioner (OAIC) of the privacy policies of 40 General Practice (GP) clinics against Australian Privacy Principle (APP) 1.

1.2 APP 1 requires entities that are subject to the Privacy Act (APP entities), including health service providers, to have a clearly expressed and up-to-date privacy policy describing how they manage personal information. An effective privacy policy forms the basis for good privacy management within APP entities.

1.3 The purpose of the assessment was to assist GP clinics to improve or enhance their existing privacy policy, taking into account the requirements under the Privacy Act 1988 (Privacy Act).

1.4 The assessment also aimed to enhance the GP clinics’ understanding of privacy and their obligations under the Privacy Act and, where relevant, the My Health Records Act 2012 (Cth) (the My Health Records Act)\(^1\) as well as the Healthcare Identifiers Act 2010 (Cth) (HI Act).

1.5 The My Health Records Act refers to the ‘My Health Records system’ and the ‘My Health Record System Operator’. This report generally uses the terms My Health Record system and My Health Record System Operator accordingly.

1.6 The selection of 40 GP clinics was random, other than ensuring that half of the clinics were GP Super Clinics and that all of Australia’s states and territories were represented.

Objective and scope of the assessment

1.7 The assessment examined each GP clinic’s privacy policy against APPs 1.3, 1.4 and 1.5. Specifically, the assessment considered whether each entity’s privacy policy:

- was clearly expressed and up-to-date about the management of personal information (APP 1.3)
- covered the content requirements (APP 1.4)
- was available in an appropriate form (APP 1.5).

1.8 The assessment examined the content, layout and availability of the privacy policy but did not consider how the information handling procedures set out in the privacy policy were implemented in practice.

Information required

1.9 In order to conduct the assessment, the OAIC required each entity to provide:

\(^1\) At the date of the assessment the relevant Act was the Personally Controlled Electronic Health Records Act 2012 (Cth) (PCEHR Act). The changes made to that Act when it changed its name to the My Health Records Act do not affect the issues set out in this assessment.
• a copy of their privacy policy
• if the entity published their privacy policy online, a link to that policy
• a statement describing:
  o how a person could obtain a copy of the privacy policy
  o if and where the privacy policy is displayed in the GP clinic
  o whether the privacy policy is provided to all new patients attending the GP clinic
  o whether the entity had signed a participation agreement with the My Health Record system operator
  o whether the entity held individual healthcare identifiers (IHIs).

Conduct of the assessment
1.10 The assessments were conducted from the OAIC’s premises in Sydney from May to June 2015. Upon completion, the OAIC provided each entity with an individual report outlining their results and any recommendations or suggestions for improving their privacy policy.

Assessment technique
1.11 This assessment focussed on identifying the privacy risks to the effective handling of personal information by the GP clinics in accordance with relevant legislation. For more information about privacy risk ratings, refer to the OAIC’s ‘Risk based assessments – privacy risk guidance’ at Appendix A. Further detail on this approach is provided in Chapter 7 of the OAIC’s Guide to privacy regulatory action.

Summary statistics and privacy risks
1.12 This report sets out summary statistics regarding findings made in the assessments in Part 2. A discussion of the privacy risks identified in the assessments and related recommendations made are set out in Part 3. While the findings and recommendations relate to the assessed GP clinics, they contain helpful information for all GPs to consider.

Resources
1.13 As a part of this assessment, the OAIC identified a number of available resources that may assist GP clinics to understand and meet their APP 1 obligations. These are set out in Appendix B.

1.14 A number of professional bodies have provided APP 1 privacy policy templates for their members. The OAIC has been in contact with these bodies to provide feedback with the aim of improving privacy policy templates used by GPs.
Part 2 — Summary statistics regarding findings

2.1 The OAIC found that 36 GP Clinics had a privacy policy, but four out of the 40 GP clinics did not have a privacy policy that was capable of assessment against APP 1. Findings in the rest of this report refer to the 36 GP clinics assessed.

2.2 20 of 36 privacy policies covered or explicitly referred to the APPs.

2.3 Using the Flesch-Kincaid Reading Ease test, 28 of 36 policies assessed required an education of above Grade 12 to easily read and understand the policy.

2.4 Only four of the 36 privacy policies contained appropriate contact information for individuals to submit access or correction requests or make complaints to the practice.

2.5 The lack of appropriate contact details also affected whether polices had appropriate access, correction and complaint handling provisions. As a result of this, and due to other issues identified by the assessors:

- only two of the 36 policies appropriately advised patients how to make a complaint about possible breaches of their privacy
- only two of the 36 policies appropriately advised patients how they could request a correction to their personal information
- only one of the 36 privacy polices appropriately advised patients how they could request access to their personal information.

2.6 The OAIC found the policies did not contain some of the content required by APP 1.4. Our findings included:

- 18 of 36 privacy policies stated the kinds of personal information they collected and held in a manner considered to meet the requirements of APP 1.4
- 23 of 36 GP clinics stated how they generally collect personal information
- 24 of 36 GP clinics stated how they generally hold personal information
- only seven GP clinics stated how they collected and held personal information in a manner considered to meet the requirements of APP 1.4
- 20 of 36 privacy policies stated the purposes as to why they collected, held, used and disclosed personal information in a manner considered to meet the requirements of APP 1.4
- 25 of 36 privacy policies described the reasonable steps the practice took to protect patients’ personal information
- 6 of 36 privacy policies advised patients how the clinic generally would deal with a privacy complaint they received
- 31 of 36 GP clinics have signed a PCEHR Participation Agreement. Only one of the GP clinics specifically referred to the collection, use or disclosure of personal information by GPs through the use of the My Health Record system
• 33 of 36 GP clinics stated that they held IHIs. 12 privacy policies specifically referred to the collection, use or disclosure of IHIs

• No privacy policy specifically referred to the collection, use or disclosure of personal information using an electronic transfer of prescriptions service, which are systems commonly used by GPs.

2.7 19 of the 36 privacy policies did not make any statement relating to overseas disclosures. The majority of those that did refer to overseas disclosures noted that any such disclosure would only be made with the consent of the patient.

2.8 28 GP clinics had a web presence. Of these, 17 published their privacy policy online.

2.9 GP clinics provided access to privacy policies in different ways:

• 35 of 36 GP clinics provided a hard copy of their privacy policy to patients on request

• 30 of 36 GP clinics displayed information about the privacy policy in their practice

• 20 of 36 GP clinics provided a copy of their privacy policy to all new patients who attend their clinic.
Part 3 — Detailed commentary

APP 1.5 — Availability and accessibility

Background

3.1 APP 1.5 says an entity must take such steps as are reasonable in the circumstances to make its privacy policy available in such form as is appropriate. The APP guidelines\(^2\) set out that an APP entity must:\(^3\)

- take reasonable steps to make its privacy policy available free of charge and in an appropriate form (usually on its website)
- upon request, take reasonable steps to provide a person or body with a copy of its privacy policy in the particular form requested.

Commentary and recommendations

3.2 The assessment results relating to APP 1.5 showed:

- 35 of 36 GP clinics provided a hard copy of their privacy policy to patients on request
- 30 of 36 GP clinics displayed information about the privacy policy in their practice
- 20 of 36 GP clinics provided a copy of their privacy policy to all new patients who attend their clinic
- 17 out of 28 GP clinics (that had a web presence) published their privacy policy online.

3.3 Where GP clinics had a web presence, the OAIC took the view that the policy should be available on the website, and made that recommendation. If a clinic had their privacy policy on their website in non-HTML format, a suggestion was made that the policy be published in HTML format.

3.4 In addition, as patient interaction with a GP clinic is predominately face to face rather than over the web, the assessors took a view that GP clinics should make the privacy policy available to their patients at the clinic.

3.5 If the GP clinic did not display the privacy policy at their clinic nor hand a copy to new patients, then a recommendation was made that they implement at least one of the following steps:

- display the privacy policy prominently at the practice, and keep copies of the privacy policy available
- hand a copy to all new patients when they register

\(^2\) The [APP guidelines](#), published by the OAIC outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters we may take into account when exercising functions and powers under the Privacy Act.

\(^3\) APP guidelines, [Chapter 1: APP 1 — Open and transparent management of personal information, Key points](#)
• refer to the privacy policy (and how to obtain a copy) in registration forms, collection notices and other consent forms.

**APP 1.3 — Readability and currency**

**Background**

3.6 APP 1.3 states that an APP entity must have a clearly expressed and up-to-date privacy policy about how it manages personal information.

3.7 The assessors tested readability using the Flesch-Kincaid Reading Ease test as found at [www.read-able.com](http://www.read-able.com). This test analyses text, and provides an estimated education grade and reading age required by readers to easily understand the text. Use of this test allowed the assessors to take a relative view of readability across the policies assessed. The assessors also applied their own view of the readability of the policies, including the use of headings, sentence lengths and complex words.

3.8 The average word count of privacy policies was 1,318 and the median length was 1,083 words.

**Commentary and recommendations**

3.9 Generally, the policies required a high reading age to easily understand them, with 30 of the 36 privacy policies requiring an assumed education level of above grade 12. The table below breaks down the average reading age required to be able to easily understand the policy by number of policies:

<table>
<thead>
<tr>
<th>Age</th>
<th>Reading Level required to read the APP Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-17 years</td>
<td>2</td>
</tr>
<tr>
<td>17-18 years</td>
<td>4</td>
</tr>
<tr>
<td>18-19 years</td>
<td>6</td>
</tr>
<tr>
<td>19-20 years</td>
<td>8</td>
</tr>
<tr>
<td>20-21 years</td>
<td>10</td>
</tr>
<tr>
<td>21-22 years</td>
<td>12</td>
</tr>
<tr>
<td>22-23 years</td>
<td>8</td>
</tr>
<tr>
<td>23-24 years</td>
<td>6</td>
</tr>
</tbody>
</table>
3.10 The APP guidelines state ‘[a]t a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity’.  

3.11 Where the test showed a required average age of 17-18 or 18-19 years to easily understand the privacy policy, we recommended that GP clinics review their policy to see if it could be made easier to read. For reading ages above that, a recommendation was made that the GP clinic should review and amend their privacy policy, so that it is more clearly expressed and made easier to understand.

3.12 20 of 36 privacy policies covered or explicitly referred to the APPs. 11 of 36 privacy policies indicated they had been reviewed after 12 March 2014 (the date the APPs came into effect).

3.13 Where GP clinics did not specifically mention or deal with the APPs, the OAIC recommended that the GP clinics amend their privacy policy so that it reflects the APPs.

3.14 12 of 36 privacy policies contained material not relevant to APP 1 and the management of personal information. For example, a privacy policy may state that the ‘...practice follows the guidelines of the Handbook for the Management of Health Information in Private Medical Practice’. Without further explanation, information of this kind will not directly assist patients to know how their personal information will be handled by the practice.

3.15 In the interests of only including information that assists patients to understand how their information is handled and to keep the policies to a manageable length, clinics were advised to remove material of this nature.

APP 1.4 — Contactability

Background

3.16 A privacy policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)).

3.17 Interpreting the law, the APP Guidelines say that at a minimum, the privacy policy should state the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).

---

4 APP Guideline [1.8]
5 This was a reference to a previous resource of the Royal Australian College of General Practitioners which has since been replaced by the Handbook for the management of health information in general practice (3rd edition)
6 APP Guideline [1.22]
Commentary and recommendations

3.18 Only four of 36 privacy policies contained contact information as described in the APP guidelines.

3.19 Privacy policies should contain the same contact details when explaining how an individual can complain about an APP entity’s breach of the APPs.7

3.20 Where the privacy policies did not contain sufficient contact details as outlined by the APP guidelines, a recommendation was made that the policies be updated accordingly. While most policies contained some form of contact details, they generally were not privacy specific contact details, or did not contain all the minimum details outlined in the APP guidelines.

3.21 This issue had a flow on effect when policies were assessed against APP 1.4, for their content relating to an individual’s right to access or correct their personal information or make a complaint for breach of privacy (see below).

APP 1.4 — Content: Collection, holding, use and disclosure of personal information

Background

3.22 The content requirements for a privacy policy relating to the collection, holding, use and disclosure of personal information are set out in APP 1.4(a), (b), (c), (f) and (g). A privacy policy must include:

- the kinds of personal information collected and held
- how personal information is collected and held
- the purposes for which the entity collects, holds, uses and discloses personal information
- whether the entity is likely to disclose personal information to overseas recipients and, if so, the countries in which such recipients are located (if that is practicable).

3.23 The OAIC guidelines provide further guidance on these issues at paragraphs 1.15 to 1.24 and 1.28 to 1.32.

Commentary and recommendations

3.24 GP clinics appeared to find this the most difficult requirement to address and were not fully complying with their obligations for a variety of reasons.

3.25 Although 30 of 36 privacy policies referred specifically to the collection, use or disclosure of government identifiers (such as Medicare numbers), overall the assessors determined that only 18 of the privacy policies stated the kinds of personal information they collected and held in a manner that met the requirements of APP 1.4.

---

7 See APP Guidelines [1.26]
3.26 The other policies generally provided only brief information about the kinds of personal information they collected, attempting to cover it in a short statement, such as collecting information ‘...that is relevant to [the patient’s] medical care’.

3.27 A recommendation was made that the policies include further details of the kinds of personal information being collected, such as the patient’s name, date of birth, address (and where missing, Medicare number or individual healthcare identifiers).

3.28 13 policies did not provide sufficient information about how the clinic collected personal information. For instance, polices were missing one or more usual collections, including through patient registration forms, through the consultation process or from third parties (eg other healthcare providers, pathology labs). GP clinics were asked to amend their privacy policies to reflect how they generally collected personal information.

3.29 A few of the content requirements in APP 1.4 required two or more elements to be addressed. If one element was missing, then the GP clinics were asked update their policies to reflect that missing element.

3.30 For example, privacy polices need to state how personal information is collected and held. Broken down into each of the elements that needed addressing:

- 23 of 36 GP clinics stated how they generally collect personal information
- 24 of 36 GP clinics stated how they generally hold personal information
- seven GP clinics stated how they collected and how they held personal information.

In many cases, this issue was a technical oversight in the wording of the policy which could be easily addressed; these clinics were recommended to amend their policies.

3.31 How an entity ‘holds’ information also includes how the entity secures that information. This aspect of ‘holding’ was separately captured in the assessment. Generally clinics did reasonably well on security issues, with 25 of 36 privacy policies describing the reasonable steps the practice took to protect patients’ personal information.

3.32 However, several privacy policies provided only a general statement such as ‘information is held securely’, which the assessors considered insufficient. In these cases a recommendation was made that the policy provide high level information on the most relevant security measures the clinic had, such as the use of passwords to protect electronic information and keeping paper files in secure cabinets.

3.33 20 of 36 privacy policies stated the purposes as to why they collected, held, used and disclosed personal information in a manner the assessors considered met the requirements of APP 1.4.

---

8 see APP Guidelines [1.20]
 Whilst most privacy policies clearly stated providing healthcare as their purpose, a number did not state a range of other (usual) purposes for which the personal information might be collected, held, used or disclosed – for example for quality assurance and accreditation purposes or to be used by IT services providers.

In those instances, a recommendation was made that GP clinics clearly state all of the usual purposes for which they collect, hold, use and disclose information so that a patient would be aware of these other purposes.

Regarding overseas disclosures, 19 of the 36 privacy policies did not make any statement relating to overseas disclosures; these clinics were asked to consider this issue and amend their policy appropriately. The majority of those that did refer to overseas disclosures noted that any such disclosure would only be with the consent of the patient.

**APP 1.4 — Content: Accessing and seeking correction of personal information and making complaints**

**Background**

The content requirements for a privacy policy relating to the access to and correction of personal information and the making of complaints are set out in APP 1.4(d) and (e). A privacy policy must include:

- how a person may access and seek correction of personal information
- how an individual may complain about a breach of the APPs.

The APP guidelines state that a privacy policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state that individuals have a right to request access to their personal information, to request its correction (APPs 12 and 13) and to provide appropriate contact details.

The APP guidelines state that a privacy policy must explain how an individual can complain about an APP entity’s breach of the APPs. This should include some information on the GP clinic’s complaint handling procedure and appropriate contact details.

**Commentary and recommendations**

Only one of the 36 privacy policies appropriately advised patients how they could request access to their personal information.

Only two of the 36 privacy policies appropriately advised patients how they could request a correction to their personal information.

---

9 APP Guidelines [1.22]
10 APP Guidelines [1.25]
3.42 The low results in respect of accessing and seeking correction of personal information were strongly influenced by the lack of appropriate contact details being provided, as noted in paragraphs 3.18 to 3.21.

3.43 Only two of 36 privacy policies appropriately advised patients how to make a complaint about possible breaches of their privacy. This low result again was influenced by the lack of appropriate contact details referred to above.

3.44 Six of 36 privacy policies advised patients how the clinic generally would deal with a complaint they received. This low number was due to policies not providing sufficient information about the GP clinic’s procedure for dealing with privacy complaints.

3.45 Recommendations made included that policies be expanded to include more detail on their complaint resolution procedure, such as:

- the complaint should be made in writing
- the organisation may take a reasonable time to respond to the individual’s complaint (usually 30 days)
- the complaint can be taken to the OAIC if the individual is unsatisfied with the entity’s response.

APP 1.4 — Content: eHealth

Background

3.46 The assessment also aimed to enhance the GP clinics’ understanding of privacy in the context of their obligations under the My Health Records Act and the HI Act.

3.47 Therefore, as part of the assessment the OAIC reviewed the privacy policies to ensure GP clinics adequately covered the use of the My Health Record system and their collection and use of IHIs. The assessment also looked at the use of electronic transfer of prescriptions (eTP) services.

Commentary and recommendations

3.48 31 of 36 GP clinics had signed a PCEHR Participation Agreement. Only one of these GP clinics specifically referred to the collection, use or disclosure of personal information by GPs through the use of the My Health Record system.

3.49 33 of 36 GP clinics stated that they held IHIs. 12 privacy policies specifically referred to the collection, holding, use or disclosure of IHIs.

3.50 No privacy policy specifically referred to the collection, use or disclosure of personal information as a result of using an eTP service.

3.51 The OAIC recommended GP clinics amend their privacy policy so that:

- if the My Health Record system is used, it informs patients that the GP clinic may collect, use and disclose their health information for the purposes of using the My Health Record system
• if IHIs are collected, it informs patients that the GP clinic collects, holds, uses or discloses IHIs
• if an eTP service is used, it informs patients that the GP clinic may collect, use, hold or disclose their health information for the purposes of using that eTP service.
## Appendix A — Risk based assessments — privacy risk guidance

<table>
<thead>
<tr>
<th>Privacy risk rating</th>
<th>Entity action required</th>
<th>Likely outcome if risk is not addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High risk</strong></td>
<td><strong>Immediate management attention is required.</strong>&lt;br&gt;Entity <em>must</em>, as a high priority, take steps to address mandatory requirements of Privacy legislation or other relevant legislation</td>
<td>○ Likely breach of relevant legislative obligations (for example, APP, TFN, Credit) or not likely to meet significant requirements of a specific obligation (for example, an enforceable undertaking)&lt;br&gt;○ Likely adverse or negative impact upon the handling of individuals’ personal information&lt;br&gt;○ Likely violation of entity policies or procedures&lt;br&gt;○ Likely reputational damage to the entity, such as negative publicity in national or international media.&lt;br&gt;○ Likely adverse regulatory impact, such as Commissioner Initiated Investigation (CII), enforceable undertakings, material fines&lt;br&gt;○ Likely ministerial involvement or censure (for agencies)</td>
</tr>
<tr>
<td><strong>Medium risk</strong></td>
<td><strong>Timely management attention is expected.</strong>&lt;br&gt;Entity <em>should</em>, as a medium priority, take steps to address Office expectations around requirements of Privacy legislation or other relevant legislation</td>
<td>○ Possible breach of relevant legislative obligations (for example, APP, TFN, Credit) or meets some (but not all) requirements of a specific obligation&lt;br&gt;○ Possible adverse or negative impact upon the handling of individuals’ personal information&lt;br&gt;○ Possible violation of entity policies or procedures&lt;br&gt;○ Possible reputational damage to the entity, such as negative publicity in local or regional media.&lt;br&gt;○ Possible adverse regulatory impacts, such as Commissioner Initiated Investigation (CII), public sanctions (CII report) or follow up assessment activities.&lt;br&gt;○ Possible ministerial involvement or censure (for agencies);</td>
</tr>
<tr>
<td><strong>Low risk</strong></td>
<td><strong>Management attention is suggested.</strong>&lt;br&gt;Entity <em>could</em>, as a lower priority than for high and medium risks, take steps to better address compliance with requirements of Privacy legislation or other relevant legislation</td>
<td>○ Risks are limited, and may be within acceptable entity risk tolerance levels&lt;br&gt;○ Unlikely to breach relevant legislative obligations (for example, APP, TFN, Credit)&lt;br&gt;○ Minimum compliance obligations are being met</td>
</tr>
</tbody>
</table>
Appendix B — Resources

A number of resources are available that may assist GP clinics to understand and meet their APP1 obligations. They are as follows:

- Chapter 1 of the Australian Privacy Principles Guidelines issued by the Australian Information Commissioner regarding [APP1 — Open and transparent management of personal information](http://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information)
- Our poster on *What to look for in a privacy policy*[^14]
- The RACGP’s updated [Privacy policy template for general practices](http://www.racgp.org.au/your-practice/ehealth/protecting-information/privacy/)

The following are links to information about readability (including media releases by the OAIC containing information about readability and APP1 policies):

- [Privacy policies still have room for improvement](http://www.oaic.gov.au/media-and-speeches/media-releases/privacy-policies-still-have-room-for-improvement)

The OAIC tested the ‘readability’ of the privacy policy with the assistance of the ‘Flesh-Kincaid Reading Ease’ test (using the online test at [www.read-able.com](http://www.read-able.com)). When testing a policy we pasted the text of the policy into the test tool. The test is not conclusive, but helps give an indication of the complexity and readability of a document.