Assessment report summary
Assessment undertaken: May 2016
Draft report issued: July 2016
Summary report issued: January 2017
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Description of assessment</td>
<td>4</td>
</tr>
<tr>
<td>Background</td>
<td>4</td>
</tr>
<tr>
<td>Objective and scope</td>
<td>4</td>
</tr>
<tr>
<td>Timing, location and methodology</td>
<td>4</td>
</tr>
<tr>
<td>Summary of findings</td>
<td>5</td>
</tr>
</tbody>
</table>
Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) conducted a privacy assessment of Australian Health Practitioner Regulation Agency (AHPRA). The assessment considered AHPRA’s handling of healthcare identifiers and associated identifying information against the requirements of the Privacy Act 1988 (Cth) (Privacy Act), in particular Australian Privacy Principle (APP) 10 which relates to data quality and APP 11 which concerns security.

1.2 The OAIC’s assessment identified some data quality and security issues and made four recommendations to address these issues.

1.3 AHPRA accepted all of the OAIC’s recommendations and has implemented or is in the process of implementing the recommendations.

Description of assessment

Background

1.4 AHPRA is a national registration authority for the purposes of the Healthcare Identifiers Act 2010 (Cth) (HI Act) and assigns the majority of Healthcare Provider Identifier – Individual identifiers (HPI-Is) to healthcare providers and manages the registration of the HPI-Is and associated personal information (HI information).

1.5 The OAIC is the dedicated privacy regulator under the HI Act. In this role, the OAIC considers it important that it has oversight of the handling of HI information. The assessment is intended to provide this oversight.

1.6 The OAIC also consulted the National Health Practitioner Ombudsman and Privacy Commissioner (NHPOPC) before undertaking this assessment. The NHPOPC has general oversight of AHPRA in relation to privacy, but not specifically for HPI-Is.

Objective and scope

1.7 The objective of the assessment was to consider whether the handling of personal information by AHPRA is in accordance with the APPs found in the Privacy Act and the HI Act.

1.8 The scope of this assessment was limited to the consideration of AHPRA’s handling of HPI-Is and associated identifying information under APPs 10 (data quality) and 11 (security). The OAIC examined the relevant policies and procedures of AHPRA related to the data quality and security of personal information, and the implementation of these policies.

1.9 AHPRA is bound by the National law, which it considers its primary legislation and (at the time of fieldwork) the records management legislation of the states and territories. The OAIC did not assess AHPRA’s compliance with the National Law or the records management Acts of states and territories as they were outside the scope of this assessment.

Timing, location and methodology

1.10 The OAIC asked AHPRA to provide copies of relevant policies and procedures related to the data quality and security of personal information. The assessors then conducted the fieldwork.
The component of the assessment at AHPRA’s National office in Melbourne from 2 to 4 May 2016, which included interviewing key members of staff and reviewing further documentation.

1.11 The assessment of AHPRA was risk based. The focus was on identifying privacy risks to the effective handling of personal information in accordance with privacy legislation.

Summary of findings

1.12 The findings of the OAIC’s assessment show that AHPRA appears to have in place:

- a good privacy aware culture with a focus on making privacy a business wide concern
- good privacy governance structures which facilitate information security awareness and compliance
- an effective risk management regime which includes consideration of privacy risks and is supported by a number of external assurance activities.

1.13 However, the OAIC’s findings also identified a number of privacy risks. These include:

- Internal practices, procedures and systems - in the assessors’ opinion there is a risk that the lack of currency of ICT policies could lead to confusion and a lack of certainty regarding their application. The assessors were also informed that there were instances of different interpretations of document management and storage procedures being adopted due to the current decentralisation of operations across a number of offices across Australia. We note that AHPRA’s ICT policies are currently under review. A forecast restructure of AHPRA’s operations will also assist in making policies and procedures standard across its business.

- Access controls – the OAIC was informed that there was limited access provisioning and audit capability on specific parts of AHPRA’s ICT systems where personal information is held. The assessors note that AHPRA is aware of this risk and is working to implement short term mitigations until new systems can be implemented.

- Data quality - the quality of HIs and associated identifying information held by AHPRA might be impacted in relation to data entry errors in transcribing data from documents into its ICT systems and to inconsistencies in HI information held by AHPRA and by DHS.

- Transfer of HI information to DHS – there is a risk that personal information may be misused, interfered with or lost when it is transferred to DHS. The OAIC acknowledges that AHPRA is aware of this security risk and is pursuing longer term solutions to address this issue.

1.14 The OAIC made four recommendations to address these risks. In summary they relate to AHPRA:

- reviewing and updating its policies and procedures
- adjusting its access control practices to limit access to information to those that need access, as well as monitoring these controls
- identifying and implementing ways to improve its data entry quality assurance
- implementing additional security protocols when transferring certain HI information to DHS.

1.15 AHPRA has accepted all of the OAIC’s recommendations and has implemented or is in the process of implementing the recommendations.