Australian Government

Office of the Australian Information Commissioner

Annual report of the Information Commissioner's activities in relation to eHealth

2013–14

Protecting information rights — advancing information policy

The Office of the Australian Information Commissioner (OAIC) was established on
1 November 2010 by the *Australian Information Commissioner Act 2010.*

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the OAIC.

ISSN 2202-7262

Enquiries regarding the licence and any use of this report are welcome at:
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Tel: 02 9284 9800
TTY: 1800 620 241 (no voice calls)
Email: enquiries@oaic.gov.au

Contents

1. Executive summary

The 2013–14 financial year was the second year of operation of the Personally Controlled Electronic Health Record (PCEHR) system, established under the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act). It was also the fourth year of the Healthcare Identifiers (HI) service, a critical enabler for the PCEHR system and eHealth generally. The HI service is established under the *Healthcare Identifiers Act 2010* (Cth) (HI Act).

The handling of individuals' personal information is at the core of both the PCEHR system and the HI service (collectively referred to as eHealth in this report). In recognition of the special sensitivity of health information, both the PCEHR and HI Acts contain provisions protecting and restricting the collection, use and disclosure of personal information. The Information Commissioner oversees compliance with those provisions and is the independent regulator of the privacy aspects of the PCEHR system and HI service.

This annual report sets out the Information Commissioner's eHealth compliance and enforcement activity during 2013–14, in accordance with s 106 of the PCEHR Act and s 30 of the HI Act. The report also provides information about the Office of the Australian Information Commissioner's (OAIC) other eHealth activities, including its audit/assessment program, development of guidance material, provision of advice, and liaison with key stakeholders (including the PCEHR System Operator and HI Service Operator).

During the reporting period, the OAIC received no complaints regarding the PCEHR system, and received and closed two HI complaints. Despite minimal compliance and enforcement activity during the year, the OAIC carried out a full program of eHealth related work, including:

- commencement of five audits/privacy assessments and completion of three audits/assessments
- establishment of 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,* in consultation with the Department of Health (Health)
- providing input to the review of the PCEHR system chaired by Mr Richard Royle
- responding to two mandatory data breach notifications from the PCEHR System Operator
- reviewing and developing guidance materials for a range of health and consumer audiences

- training and development of the OAIC's staff in the eHealth privacy regulatory framework.

The OAIC's eHealth activities were carried out under a memorandum of understanding (MOU) with Health signed on 29 November 2012 and which continued to 30 June 2014. More information about the OAIC's MOU with Health is provided below in section 2 of this report. The MOU can be accessed on the OAIC's website, www.oaic.gov.au.

2. Introduction

Many Australians view their health information as being particularly sensitive. This sensitivity has been recognised in the PCEHR and HI Acts, which both contain provisions that regulate the collection, use and disclosure of information, and give the Information Commissioner a range of enforcement powers. This contributes to a strong privacy framework, providing a foundation for public confidence in the PCEHR system and HI Service.

The Information Commissioner is the independent regulator for the privacy aspects of the PCEHR system and HI service, and plays a crucial role in overseeing compliance with privacy provisions. However, the OAIC's role is not limited to compliance and enforcement. The OAIC also carries out a number of other eHealth activities under its MOU with Health.

The MOU sets out a program of work that includes business as usual activities (such as responding to requests for advice and investigating privacy complaints relating to eHealth), and project-based work (such as developing guidance materials, conducting audits/assessments and establishing complaint handling arrangements). Information about these activities is set out in sections 3 and 4 of this report. Further information about the OAIC's MOU activities can be found in Quarterly Reports under the MOU, available on the OAIC website, www.oaic.gov.au.

The MOU, signed on 29 November 2012, covers activities related to both the PCEHR system and the HI service. During 2013–14 , the OAIC received $2,406,292 from Health to carry out activities in accordance with the MOU.

2.1 The Information Commissioner's eHealth functions

The PCEHR system

The Information Commissioner's roles and responsibilities under the PCEHR Act and *Privacy Act 1988* (Privacy Act) include the following:

- respond to complaints received relating to the privacy aspects of the PCEHR system as the Commissioner considers appropriate, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Commissioner's own initiative, acts and practices that may be a contravention of the PCEHR Act in connection with health information contained in a consumer's PCEHR or a provision of Part 4 or 5 of the PCEHR Act
- receive data breach notifications and assist affected entities to deal with data breaches in accordance with the PCEHR legislative requirements
- investigate failures to notify data breaches
- exercise, as the Commissioner considers appropriate, a range of enforcement powers available in relation to contraventions of the PCEHR Act or contraventions of the Privacy Act relating to the PCEHR system, including making determinations, accepting enforceable undertakings, seeking injunctions or seeking civil penalties
- conduct audits/assessments
- issue guidelines outlining how the OAIC will approach enforcement issues under the PCEHR Act (s 111 of the PCEHR Act)
- provide a range of advice and guidance material.

Healthcare Identifiers service

The Information Commissioner has the following roles and responsibilities under the HI Act and Privacy Act:

- respond to complaints received relating to the privacy aspects of the HI service as the Commissioner considers appropriate, including through preliminary inquiries, conciliation, investigation or deciding not to investigate a complaint
- investigate, on the Commissioner's own initiative, acts and practices that may be a misuse of HIs
- receive data breach notifications and respond as appropriate
- conduct audits/assessments
- provide a range of advice and guidance material.

2.2 Year in review — a summary

During the financial year 2013–14, the OAIC undertook the following activities:

Table 1: OAIC PCEHR and HI activities 2013–14

Activity	PCEHR	HI
Telephone enquiries	6	1
Written enquiries[1]	2	1
Complaints received and finalised	0	2
Policy advices[2]	10	3
Audits/assessments[3]	5	3
Mandatory data breach notifications received	2	n/a
Media enquiries	1	0

[1] One written enquiry was received which related to both the PCEHR system and HI service. This is included in both columns.

[2] Two policy advices related to both the PCEHR system and HI service and are included in both columns.

[3] One assessment related to both the PCEHR system and HI service and is included in both columns.

3. OAIC and the PCEHR system

The OAIC performs a range of functions in relation to the PCEHR system. These functions include compliance and enforcement activities and other activities set out under the MOU, including providing privacy related advice and developing guidance and training materials for internal and external stakeholders.

Compliance and enforcement activities include receiving and investigating complaints about alleged interferences with the privacy of a consumer in relation to the PCEHR system, and conducting audits/assessments of participants in the system to ensure they are complying with their privacy obligations. Information about the OAIC's enforcement and compliance activities is set out below under section 3.1.

The OAIC is also responsible for producing statutory and regulatory guidance for consumers and other participants such as healthcare providers, registered repository operators and the System Operator. In addition, the OAIC responds to enquiries and requests for policy advice from a broad range of stakeholders about the privacy framework for the PCEHR system and the appropriate handling of PCEHR information. These activities are an important component of the OAIC's regulatory role under the PCEHR system.

To deliver these outcomes, the OAIC liaised with external stakeholders including state and territory health and privacy regulators, professional industry bodies in the health sector and consumer organisations. Information about the OAIC's activities in relation to providing advice, developing guidance material and liaison with key stakeholders is given below in section 3.2.

3.1 OAIC enforcement and compliance activities

Complaints and investigations relating to the PCEHR system

The OAIC received no complaints about the PCEHR system during 2013–14. Therefore, the Information Commissioner did not undertake any investigations or enforcement action.

Under s 40(2) of the Privacy Act the Information Commissioner also has the discretion to investigate an act or practice that may be an interference with privacy, on the Commissioner's own initiative (without first receiving a complaint from an individual). During 2013–14 , the Commissioner did not carry out any Commissioner initiated investigations (CII) into the PCEHR system. The OAIC did, however, undertake five audits/assessments relating to the PCEHR system.

Audits/assessments relating to the PCEHR system

Under the MOU with Health, the OAIC was required to conduct up to two audits/assessments of the PCEHR System Operator and up to two audits/assessments of agencies and organisations in relation to the PCEHR system before 30 June 2014.

The OAIC worked on five audits/assessments relating to the PCEHR system in 2013–14 (one of which also related to the HI service).

PCEHR System Operator

The OAIC undertook two audits of the PCEHR System Operator.

The first audit, which commenced in May 2013, considered the System Operator's policies and procedures for the collection of personal information during the PCEHR consumer registration process. The purpose of this audit was to assess whether the System Operator's policies and procedures were consistent with its obligations under Information Privacy Principles (IPPs) 1 to 3. The draft report was provided to the System Operator in December 2013, and the System Operator provided comments in February 2014. A revised draft incorporating the System Operator’s comments was provided to the System Operator in May 2014. At 30 June 2014, the OAIC was awaiting final comments from the System Operator on the audit report.

The second audit examined the storage and security of personal information held in the National Repositories Service. The objective of the audit was to consider whether the System Operator had taken reasonable steps to protect personal information held in the National Repositories Service from loss, unauthorised access, use, modification or disclosure or other misuse. The audit commenced in November 2013 and the draft report was provided to the System Operator in May 2014. At 30 June 2014, the OAIC was awaiting final comments from the System Operator on the audit report.

Assisted registration policies

This assessment reviewed the assisted registration policies of ten healthcare provider organisations undertaking assisted registration. Under the *PCEHR (Assisted Registration) Rules 2012* (Cth), organisations providing assisted registration are required to have policies in place setting out certain matters relating to the conduct of assisted registration, including the authorisation and training of employees, recording of consumer consent and processes for consumer identification. The assessment considered how these policies addressed the privacy obligations set out in Australian Privacy Principles (APP) 3 (collection) and 11 (security of personal information), relating to the collection and security of personal information. The assessment commenced in February 2014, and the draft report was provided to the System Operator in May 2014. At 30 June 2014, the OAIC was awaiting final comments from the System Operator on the assessment report.

Calvary Health Care ACT (Calvary)

This assessment reviewed Calvary’s privacy policy and privacy collection notice, including as they relate to the PCEHR system and HI service. The objective of the assessment was to assess Calvary’s privacy policy and collection notice to determine Calvary’s readiness for and compliance with the requirements under APPs 1 (open and transparent management) and 5 (notice of collection). The assessment commenced in February 2014 and was finalised in June 2014.

Western Sydney Medicare Local (WSML)

This assessment considered WSML's assisted registration practices. The objective of this assessment was to assess the extent to which WSML, in the course of conducting assisted registration, handled personal information in accordance with APP 3 (collection), APP 5 (notice of collection) and APP 11 (security of personal information). The assessment commenced in March 2014. The draft report was provided to WSML and to the System Operator in June 2014. At 30 June 2014, the OAIC was awaiting final comments from the System Operator on the assessment report.

3.2 PCEHR system advice, guidance, liaison and other activities

Advice

PCEHR enquiries

The OAIC's Enquiries Team received eight enquiries about the PCEHR system during the reporting period.

The majority of enquiries came from individuals wanting to find out more about the PCEHR system, including how to access information in the record, how to find out who has accessed a record and how to cancel a record. Where appropriate, these enquiries were referred to the System Operator's PCEHR Helpline, operated by the Department of Human Services (DHS). The OAIC also received an enquiry from a Senator about the number and status of complaints about PCEHR matters received by the OAIC.

Following the release of the report of the review of the PCEHR system, the OAIC received two enquiries from individuals concerned about the proposal to implement an opt-out participation model, instead of the current opt-in model.

Policy advice to stakeholders and members of the public

The OAIC responded to written enquiries from consumer groups, including the Australian Privacy Foundation (APF) and the Consumer eHealth Alliance (CeHA). The APF raised a number of issues relating to privacy aspects of the PCEHR system, including general concerns about the PCEHR system and concerns about the practices of a particular health service provider. CeHA raised concerns with the OAIC regarding the accuracy of pharmaceutical benefits information contained in the PCEHR system and the use of myGov in the PCEHR registration process. CeHA also sought information about the OAIC's publication of quarterly reports under the MOU with Health. The OAIC provided advice to APF and CeHA clarifying the privacy aspects of the PCEHR system, and directed both organisations to further information where relevant.

The OAIC also responded to two enquiries from a Medicare Local about whether there would be any changes to requirements for secure messaging and PCEHRs following the commencement of reforms to the Privacy Act on 12 March 2014.

In total, the OAIC provided ten policy advices to individuals and entities about privacy and the PCEHR system.

Policy advice to the Department of Health

Under its MOU with Health, the OAIC liaises and coordinates with the PCEHR System Operator on privacy related matters, including by providing feedback and advice on proposals and projects with a possible privacy impact.

During the reporting period, the OAIC:

- provided feedback to Health on a new 'essential information' brochure to be used in a streamlined registration process in Medicare offices
- provided feedback to Health on draft versions of collection notices to be provided to consumers registering to use the PCEHR system (these notices are intended to meet Health's obligations under APP 5)
- liaised with Health regarding possible privacy risks associated with assisted registration
- liaised with Health about media reports and other issues relating to registration and use of the system by consumers and providers
- provided information to Health about potential privacy implications of a transition to an opt-out participation model.

Submissions

The OAIC provided a submission to the review of the PCEHR system in November 2013. This brief submission outlined the OAIC's role in the system and offered to discuss any privacy considerations relating to possible changes to the system with the review panel.

PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013

On 20 June 2013, the *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013* (Enforcement Guidelines) were registered on the Federal Register of Legislative Instruments. The Enforcement Guidelines were made under s 111 of the PCEHR Act, which requires the Information Commissioner to formulate, and have regard to, guidelines regarding the exercise of the Information Commissioner's powers under the PCEHR Act or a power under another related Act, such as the Privacy Act.

Amendments to the Privacy Act that took effect on 12 March 2014 granted the Information Commissioner additional enforcement powers. The OAIC has commenced a revision of the Enforcement Guidelines to include information about the new powers under the Privacy Act. Consultation on the revised Enforcement Guidelines will occur in 2014–15.

Guide to mandatory data breach notification under the PCEHR Act

In 2013–14, the OAIC continued to develop a guide to mandatory data breach notification in the PCEHR system. The draft guide explains the breach notification obligations that apply to registered repository operators (RROs), registered portal operators (RPOs) and the PCEHR System Operator under s 75 of the PCEHR Act. The guide contains information about the types of breaches that have to be reported and what information should be included in a notification. It also outlines how entities should contain a breach, evaluate risks arising from the breach and take steps to prevent future breaches.

During the reporting period, the OAIC received two mandatory data breach notifications from the System Operator (discussed in more detail below), which informed the further development of the guide. The OAIC also sought external advice on aspects of the draft guide. The OAIC expects to publish the final guide early in 2014–15.

The OAIC also developed a web based 'smart form' for data breach reporting, to assist RROs, RPOs and the System Operator to easily report matters to the OAIC and comply with their reporting obligations. The OAIC expects to release the form for use early in 2014–15.

Guidance for healthcare providers

The OAIC is currently developing guidance materials for healthcare providers about privacy and the eHealth system, to complement existing consumer resources. Consultation on the draft resources will occur in 2014–15 and key stakeholder groups will be engaged for comment.

Review of existing resources

The OAIC has commenced a review of existing PCEHR resources, which are being revised to ensure that they reflect the current functionality of the PCEHR system as well as changes to the Privacy Act (where relevant). Resources will be progressively updated in 2014–15 as required.

Liaison

Liaison with the System Operator

The PCEHR System Operator is the Secretary of Health. The OAIC has met regularly with Health in 2013–14 to discuss MOU activities and other matters relating to the PCEHR system.

In 2013–14, the OAIC finalised an *Agreement for information sharing and complaint referral relating to the personally controlled electronic health (eHealth) record system between the OAIC and the System Operator* (the Agreement), in consultation with Health. The purpose of the Agreement is to work towards ensuring that the process for making a complaint about the PCEHR system is as seamless as possible for individuals, thus avoiding a situation where complainants are needlessly referred back and forth between regulators. To this end, the Agreement aims to facilitate cooperation between the OAIC and the System Operator and remove barriers to effective complaint handling.

The Agreement also fulfils the OAIC's obligation under the MOU with Health to 'develop and agree on a protocol for processes, procedures and service standards with the PCEHR System Operator for the exchange of information and advice in relation to complaints about the PCEHR system and referral of privacy complaints and complex privacy enquiries'.

The OAIC consulted with Health on the content of the draft Agreement, and Health confirmed its acceptance of the Agreement in December 2013. The Agreement is available on the OAIC website.

Liaison with state and territory regulators

During 2013–14, the OAIC's engagement with state and territory regulators was guided by the *Information Sharing and Complaint Referral Arrangements for the Personally Controlled Electronic Health (eHealth) Record System between the OAIC and State and Territory Health and Privacy Regulators* (the Arrangement), which was developed in 2012–13. In April 2014, the Information and Privacy Commissioner New South Wales agreed to become a party to the Arrangement, joining the other parties:

- OAIC
- Office of the Information Commissioner, Queensland
- Health Services Commissioner, ACT Human Rights Commission

- Office of the Health Services Commissioner, Victoria
- South Australian Health and Community Services Complaints Commissioner.

The terms of the Arrangement include a review of the Arrangement by 30 June 2014 (and every two years subsequently). In May 2014, the OAIC wrote to all parties to the Arrangement seeking comment on the Arrangement. None of the parties indicated that any changes were required, and the OAIC wrote to all parties in June 2014 confirming that the Arrangement would continue in its current form.

Liaison with other key stakeholders

During 2013–14, the OAIC met with the National E-Health Transition Authority in order to share information and receive updates regarding the PCEHR system. The OAIC also visited the PCEHR system 'clean room' and the Sydney data centre hosting the PCEHR system to increase the OAIC's understanding of security and back-up mechanisms in place for protection of PCEHR system data.

The OAIC also met with the Safety in eHealth area of the Australian Commission on Safety and Quality in Health Care regarding their PCEHR clinical audits program.

The OAIC's Assistant Commissioner, Regulation and Strategy gave a presentation to the PCEHR Independent Advisory Council in November 2013, outlining the OAIC's activities relating to the PCEHR and HI systems.

Engagement with other key stakeholders, such as consumer groups and health organisations, occurred through responses to requests for policy advice.

Other activities

Establishing internal expertise and reference materials

Throughout 2013–14, the OAIC continued to develop its internal expertise relating to its functions and powers in connection with the eHealth system.

During the reporting period, the OAIC continued work on an internal guide to enforceable undertakings, which will form part of a broader suite of documents on the OAIC's regulatory powers. The OAIC also developed internal briefing papers on PCEHR policy issues and international eHealth models.

The OAIC also took steps to ensure that staff were fully trained in matters relating to eHealth enforcement. OAIC staff involved in conducting eHealth audits under the MOU participated in training on auditing fundamentals in November 2013, while OAIC staff from Regulation and Strategy, Dispute Resolution and Legal Services participated in a two day training session on the PCEHR Act, delivered by the Australian Government Solicitor (AGS) on 31 July and 1 August 2013.

Receiving data breach notifications

The OAIC received two mandatory data breach notifications under s 75 of the PCEHR Act.

The OAIC was advised by the System Operator of the first data breach in December 2013. This data breach involved a technical change made to the system that meant that healthcare providers could view consumers' personal health notes. Investigations by the System Operator identified the cause and a technical fix was put in place to prevent further access. The OAIC reviewed the information provided by the System Operator in relation to the breach and determined that the response was appropriate and that no further action was required.

The System Operator notified the OAIC of the second data breach in May 2014. This breach involved consumers logging into their MyGov account and using their identify verification code (IVC) to access their own PCEHR and link their PCEHR to their MyGov account. In some instances they also accidentally set up access to another consumer's PCEHR while still logged into their own MyGov account, linking that second consumer's PCEHR to their own MyGov account. This resulted in the landing page of the first consumer's PCEHR showing two 'Open your eHealth record' buttons, which provided links to open both consumers' PCEHRs. The System Operator advised that containment strategies had been implemented to prevent similar incidents occurring. It should be noted that the cause of the breach was not related to MyGov. The OAIC sought further information from the System Operator about its response to the breach. The OAIC's consideration of the data breach notification and the further information provided by the System Operator was ongoing at 30 June 2014.

The OAIC liaised with Health about other incidents relating to the PCEHR system which did not meet the criteria for mandatory data breach notifications under the PCEHR Act. In one of these incidents, an email containing a consumer's IVC and other personal information was sent to the incorrect email address. The email recipient, however, did not have the other information required to access the consumer's record. The OAIC provided recommendations to the System Operator about how it could reduce the impact of any future incidents of this type. The System Operator advised that it had implemented the OAIC's recommendations.

The OAIC also sought legal advice from AGS to clarify the threshold for mandatory notification of data breaches.

4. OAIC and the Healthcare Identifiers service

The HI service has been established as a foundation service for a range of eHealth initiatives in Australia, in particular, the PCEHR system. Accordingly, the use of healthcare identifiers has increased since the launch of the PCEHR system on 1 July 2012. Under the PCEHR system, healthcare identifiers:

- are used to identify consumers who register for a PCEHR
- enable the PCEHR System Operator to authenticate the identity of all individuals who access a PCEHR and record activity through the audit trail
- help ensure the correct health information is associated with the correct consumer's PCEHR.

In addition, registration with the HI service is a prerequisite for a healthcare provider organisation to be registered for the PCEHR system.

During the reporting period, the need for the OAIC to undertake compliance and enforcement action has been low. This has meant that the OAIC has focused on undertaking proactive compliance activities, including monitoring developments in eHealth and conducting audits/assessments.

4.1 OAIC compliance and enforcement activities

Complaints relating to the HI service

The OAIC received and finalised two related complaints about the HI service in 2013–14.

In the first complaint, the complainant alleged that the respondent, a state healthcare provider, had inappropriately accessed the complainant's individual healthcare identifier (IHI) on multiple occasions. The complainant believed that the IHI had been accessed inappropriately and because they had not received any services from the healthcare provider due to the frequency of access during a short period. The respondent in this complaint advised that the access occurred as part of testing to identify an effective process by which patient identity data could be matched with data held by the

HI service. The OAIC considered that this was a permitted use of an IHI under the HI Act, as the access was for the purpose of managing health information. The OAIC closed the complaint on the basis that the healthcare provider had not breached the HI Act.

In the second complaint, the same complainant alleged that the respondent, an Australian Government department, had collected the information accessed by the first respondent and used it in the assessment of a case concerning the complainant. The OAIC closed this complaint on the basis that the complainant had not first complained to the agency that was the subject of the complaint.

Investigations relating to the HI service

No complaint investigations or CIIs were commenced or finalised during the reporting period. At 30 June 2014, there were no HI investigations open.

Audits/assessments relating to the HI service

Under the OAIC's MOU with Health, the OAIC was required to conduct up to two audits/assessments of the HI Service Operator (DHS-Medicare) and up to two audits/assessments of agencies, organisations or state and territory authorities during the period covered by the MOU (2012–14).

The OAIC undertook work on three audits/assessments relating to the HI service in 2013–14 (one of which also related to the PCEHR system).

HI Service Operator

The OAIC undertook two audits of the HI Service Operator.

The first audit, which commenced in May 2013, focused on the Service Operator's collection, use and disclosure of IHIs and Healthcare Provider Identifiers-Individual (HPI-I) and associated identifying information. The purpose of the audit was to assess whether the Service Operator's handling of HI information was in accordance with the IPPs, the HI Act and the *Healthcare Identifiers Regulations 2010* (Cth) (HI Regulations). The audit was finalised in April 2014.

The second audit considered the storage and security of personal information held on the database of HPI-Is. The objective of this audit was to assess the extent to which the Service Operator maintained records in accordance with the IPPs, specifically IPP 4, and the relevant terms of the HI Act and the HI Regulations which relate to the storage and security of personal information pertaining to HPI-Is. The audit commenced in October 2013 and was finalised in June 2014.

Calvary Health Care ACT (Calvary)

As outlined above in the summary of PCEHR system audits/assessments, this assessment reviewed Calvary’s privacy policy and privacy collection notice, including as they relate to the PCEHR system and HI service. The objective of the assessment was to assess Calvary’s privacy policy and collection notice to determine Calvary’s readiness for and compliance with the requirements under APPs 1 and 5. The audit commenced in February 2014 and was finalised in June 2014.

4.2 Healthcare Identifiers advice, liaison and other activities

Advice

The OAIC responded to specific requests for advice. In total, the OAIC provided three policy advices relating to the HI service, including to a Medicare Local and to the Northern Territory Department of Health. In addition, the OAIC’s Enquiries Team received two enquiries relating to the HI service during the reporting period.

Guidance

Review of existing resources

The OAIC has commenced a review of existing HI resources, which are being revised to ensure that they reflect the current functionality of the HI service as well as changes to the Privacy Act (where relevant). Resources will be progressively updated in 2014–15 as required.

As part of this review, the OAIC considered whether it should issue any additional guidance on the HI service, and determined that no additional guidance was required.

Liaison

The OAIC continued to engage with key stakeholders and provide policy advice on privacy aspects of the HI Act. This included meeting with Health on a quarterly basis under the MOU and meeting with DHS in relation to the HI service audit program.

The OAIC also met with the Australian National Audit Office to discuss its audit of Medicare customer data, including before the commencement of the audit to ensure that there was no overlap with the OAIC’s planned audits of the HI Service Operator, and to discuss the outcomes of the audit.

Other activities

Internal training

As noted above, the OAIC took steps to ensure that staff were fully trained in matters relating to eHealth enforcement. OAIC staff involved in conducting HI audits under the MOU participated in training on auditing fundamentals in November 2013.

Professor John McMillan
Australian Information Commissioner

Date: 9 September 2014