Australian Government

Office of the Australian Information Commissioner

October 2017

# Guide to mandatory data breach notification in the My Health Record system

www.oaic.gov.au

| Version | Currency dates | Changes and other comments |
|---|---|---|
| v1.0 | September 2015 to October 2017 | |
| v2.0 | October 2017 | • Text amended to reflect changes to the My Health Records Act 2012, as conferred by the Health Legislation Amendment (eHealth) Bill 2015, including changes to:<br>○ updated My Health Record data breach coverage, requirements and processes<br>○ terminology, section references and references to the Regulatory Powers (Standard Provisions) Act 2014<br>○ reference the a broader Notifiable Data Breaches scheme which will apply in Australia from 22 February 2018<br>• Minor restructuring of guide, and redrafting of text to aid with readability<br>• Additional examples provided to clarify the operation of the provisions. |

# Contents

# Introduction

This guide provides details of the mandatory data breach notification obligations under the *My Health Records Act 2012* (Cth) (My Health Records Act).

This guide is intended for use by entities covered by the My Health Records Act data breach provisions, including the My Health Record System Operator, registered healthcare provider organisations, registered repository operators, registered portal operators and registered contracted service providers.

This guide is not legally binding. However, it does set out the legislative requirements for reporting and responding to a data breach involving the My Health Record system. This guide also sets out the steps that must be taken once an entity becomes aware of certain My Health Record data breaches and will assist the relevant entities to meet their regulatory obligations in relation to the My Health Record system.

## The My Health Record system and data breach notification

The My Health Record system, established by the My Health Records Act,[1] is designed to facilitate access, by the healthcare recipient and treating healthcare providers, to a summary of health information about a healthcare recipient. The information is drawn from a number of different sources with healthcare recipients controlling what information is included on their record and who may access it.

In recognition of the special sensitivity of health information, the My Health Records Act makes it mandatory for certain entities (outlined below under Who should use this guide?) to notify the Office of the Australian Information Commissioner (OAIC) and the My Health Record System Operator of a data breach involving the My Health Record system. The My Health Record System Operator is the Australian Digital Health Agency.

The My Health Records Act also requires relevant entities to take a number of steps as soon as practicable after becoming aware of a My Health Record data breach. These steps differ slightly depending on the whether the data breach has occurred or may have occurred.

Further information on the legislative framework and regulatory approach for data breach notification is set out in Appendix C.

## Who should use this guide?

This guide is for:

- the My Health Record System Operator
- registered healthcare provider organisations
- registered repository operators (RROs)
- registered portal operators (RPOs)

[1] Prior to 26 November 2015, the My Health Records Act was called the *Personally Controlled Electronic Health Record Act 2012* (Cth) and the My Health Record system was called the Personally Controlled Electronic Health Record system.

- registered contracted service providers.

It explains how these entities can meet their mandatory data breach notification obligations under the My Health Records Act.

## What is the purpose of data breach notification?

Providing notification in the case of a data breach involving personal information is consistent with good privacy practice. Notification allows affected healthcare recipients to take any necessary action to protect their information and to ensure the ongoing security and integrity of, and confidence in, the My Health Record system. This recognises the sensitivity of the information the system contains.

The requirements imposed on reporting entities by the My Health Records Act aim to ensure that breaches are dealt with effectively and are prevented in the future.

Breach notification provides an important feedback loop for the System Operator's maintenance of system security, and enables swift containment of a breach and preventative action. It also ensures that oversight bodies (such as the OAIC) are made aware of a breach and can investigate the matter where appropriate.

## What is the purpose of notifying the OAIC?

The OAIC regulates the handling of personal information under the My Health Record system by individuals, Australian Government agencies, private sector organisations and some state and territory agencies (in particular circumstances). By notifying our office, you allow us to determine the seriousness of the breach and decide whether an investigation is warranted. This is also an opportunity for you to explain to the OAIC what steps you have taken, or are taking, to contain the breach. With this information, the OAIC will be better equipped to provide advice on responding to the breach, and to address questions and complaints directed to our office from concerned members of the public.

More information about what information should be included in a notification to the OAIC can be found in Part 2. To find out more about the role of the OAIC, see Part 5.

## What is the purpose of notifying the System Operator?

By notifying the System Operator of a breach, you allow it to determine whether it needs to take corrective actions to help mitigate any loss or damage that may result from the breach. This ensures a coordinated approach to dealing with the breach. Depending on the nature of the breach, it may also allow the System Operator to warn other registered healthcare provider organisations, RROs, RPOs and registered contracted service providers of a possible data security threat. Notifying the System Operator also then allows the System Operator to notify the affected healthcare recipients or the general public as required so they can take any necessary steps to protect their information.

## What is the purpose of the System Operator notifying affected healthcare recipients?

The purpose of notifying affected healthcare recipients of a breach is first and foremost to keep healthcare recipients informed of how they may have been affected by a breach, and to enable them to

take steps to mitigate any risks. Being open and transparent with individuals about the handling of their personal information is recognised as a fundamental privacy principle.[2]

The System Operator is responsible for notifying affected healthcare recipients of a data breach, where this is required. To be effective, breach notification to healthcare recipients should include an explanation what has been done to try to avoid or remedy any confirmed or potential harm. Where personal information has been compromised, notification can be essential in helping healthcare recipients to regain control of that information.

# More information

## Protecting personal information

For more information about how to protect personal information, including through the development of a data breach response plan, see the OAIC's *Guide to securing personal information*.

## Voluntary data breaches

The OAIC encourages entities to voluntarily report data breaches that are not covered by the mandatory data breach notification requirements of the My Health Records Act. Agencies or organisations wishing to report a data breach to the OAIC should consult the OAIC's voluntary data breach notification guide, *A guide to handling personal information security breaches* and the data breach smartform (once available).

## Notifiable data breaches scheme

On 22 February 2018, the broader Notifiable Data Breaches (NDB) scheme will commence. This broader scheme will apply to organisations covered by the *Privacy Act 1988* (Privacy Act), including private health service providers. Further information on the NDB scheme is set out below under the heading 'The broader Notifiable Data Breaches scheme'.

[2] See the 'openness principle' in the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013). This principle is reflected in Australian Privacy Principle (APP) 1 in the *Privacy Act 1988* (Cth).

# Part 1: Notifiable data breaches

This part of the guide explains in more detail what a data breach is under the My Health Records Act, and gives some examples.

## Under the My Health Record system, what is a data breach?

Under s 75 of the My Health Records Act, there are three types of data breaches:

1. a person has or may have contravened the My Health Records Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record

2. any event that has, or may have, occurred (whether or not involving a contravention of the My Health Records Act) that compromises, may compromise, has compromised or may have compromised the security or integrity of the My Health Record system or

3. any circumstances that have, or may have arisen (whether or not involving a contravention of the My Health Records Act), that compromise, may compromise, have compromised or may have compromised the security or integrity of the My Health Record system.

## Who is required to report a data breach?

Mandatory data breach notification obligations under the My Health Records Act apply to:

- the My Health Record System Operator
- registered healthcare provider organisations
- registered repository operators (RROs)
- registered portal operators (RPOs)
- registered contracted service providers.

(referred to in this guide collectively as 'reporting entities').

## When are they required to report the breach?

When a reporting entity both:

- becomes aware that such a data breach has, or may have, occurred (i.e. this requirement applies to data breaches that have been confirmed as well as to data breaches that are suspected, but have not yet been confirmed) and

- the data breach directly involved, may have involved or may involve the entity.

Reporting entities must also take certain actions in response to a breach, including notifying the relevant regulator as soon as practicable after becoming aware of the breach.

**What is a '*notifiable* data breach'?**

In this guide a 'notifiable data breach' refers to a data breach that meets the criterion set out under s 75(1) of the My Health Records Act, so that it must be reported to the relevant regulator.[3] Depending on the circumstances, where there is a notifiable data breach, there may or may not be an additional requirement to notify a healthcare recipient of the breach. More information about the circumstances in which affected healthcare recipients will be notified of a data breach is set out in Part 2 and Part 3.

## To whom must they report the breach?

Slightly different notification obligations apply for different types of entities.

The System Operator must report a notifiable data breach to the OAIC. The System Operator is also responsible for notifying affected healthcare recipients of a breach where this is required by the My Health Records Act. For more information about the System Operator's breach notification obligations, see Part 4.

For other reporting entities, notification requirements differ depending on whether the entity

- Is NOT a state or territory authority or instrumentality of a state or territory:
    - in which case they must report a notifiable data breach to the OAIC and the System Operator.[4] Guidance on the notification requirements for these entities is given in Part 3.
- IS a state or territory authority or instrumentality of a state or territory:
    - in which case they must report a notifiable data breach to the System Operator but not to the OAIC. State and territory entities may also voluntarily report data breaches to their local privacy regulator in addition to reporting to the System Operator.

Even though state and territory entities are not required to report data breaches to the OAIC, this guide is still useful for them as it can provide best practice guidance on how to prepare for and report a data breach in the My Health Record system.

## What is an unauthorised collection, use or disclosure?

Part 4 of the My Health Records Act specifies when a collection, use or disclosure of health information in a healthcare recipient's My Health Record is authorised.[5] This includes collection, use and disclosure by a participant in the My Health Record system:

[3] The My Health Records Act does not use the term 'notifiable data breach'.

[4] See s 75(2) of the My Health Records Act.

[5] Many of the authorisations set out below do not extend to health information that meets the definition of a healthcare recipient-only note in the My Health Records Act. For instant, these could include notes made by the healthcare recipient to help them remember things such as complementary medicines and general health.

- for the purpose of providing healthcare to the healthcare recipient (in line with access controls set by the healthcare recipient or default access controls as applicable) (s 61)
- to a healthcare recipient nominated representative (in line with access controls set by the healthcare recipient or default access controls as applicable) (s 62)
- for the management or operation of the My Health Record system, if the healthcare recipient would reasonably expect it to be handled for that purpose, or in response to a request by the System Operator for the purpose of performing a function of the System Operator (s 63)
- in the case of a serious threat to an individual's life, health or safety or to public health or public safety (provided certain conditions are met) (s 64)
- where required or authorised by another law (s 65)
- of health information included in a My Health Record for any purpose:
    - to the healthcare recipient (s 66)
    - to someone other than the healthcare recipient, with the healthcare recipient's consent (s 66)
- by the healthcare recipient (with regard to their own information) (s 67)
- for purposes relating to the provision of indemnity cover for a healthcare provider (s 68).

The My Health Records Act also authorises the System Operator to disclose health information in the following circumstances:

- to a court or tribunal when ordered or directed by the court or tribunal (s 69)
- for certain law enforcement purposes (s 70).

Any collection, use or disclosure of health information included in a healthcare recipient's My Health Record within the My Health Record system that is not covered by these provisions will be unauthorised. For the reporting entities, an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record is a notifiable data breach that must be reported.

Unauthorised uses may include improperly accessing, viewing, modifying or deleting information included in a healthcare recipient's My Health Record.[6]

**Example**
Dr Blyton is a GP who is authorised by her registered healthcare provider organisation to use the My Health Record system. One evening, Dr Blyton searches the system to see if her neighbour, a high-profile sports star who is a patient at the clinic, has a record. She finds the neighbour's record and – as her neighbour has not set access controls – views the information in it, including his MBS data and a file uploaded by a psychologist.

Viewing information in an individual's My Health Record is considered a 'use' of information. As Dr Blyton used the information in her neighbour's record and it was not for the purposes of providing healthcare to her neighbour, she has breached s 59 of the My Health Records Act.

[6] See definition of 'use' under s 5 of the My Health Records Act.

When Dr Blyton's neighbour next logs on to his My Health Record, he notices that the audit log shows that Dr Blyton accessed his record. He calls up the healthcare provider organisation to ask why Dr Blyton has accessed his record. As soon as the healthcare provider organisation becomes aware that Dr Blyton has accessed her neighbour's record for purposes unrelated to providing healthcare, it is required to comply with the data breach notification requirements of s 75 of the My Health Records Act.

In addition, Dr Blyton may be subject to a civil or criminal penalty under the My Health Records Act.

## What is a compromise of the security or integrity of the My Health Record system?

Under the My Health Records Act reporting is required where:

- an event or circumstance *has* occurred or arisen OR an event or circumstance *may have* occurred or arisen

AND

- the event or circumstance *has* compromised the security or integrity of the system OR the event or circumstance *may have* compromised the security or integrity of the system.

The event or circumstance must be reported even if there has not been an actual or potential contravention of the My Health Records Act.

An event or circumstance that may compromise the security or integrity of the My Health Record system include those situations that expose or place at risk (or may expose or may place at risk) the features of the My Health Record system that go to the ongoing operation of the system and the protections of the records contained in the system. The My Health Records Act defines the 'My Health Records system' more widely than the database holding individual My Health Records. See the glossary for the full definition.

**Example**
A registered healthcare provider organisation discovers that an external party has hacked into its IT system. As its IT system connects to the My Health Record system, there is a possibility that the files allowed the hacker to use the organisation's credentials to log in to the My Health Record system and access information in the system.

This would be considered a circumstance that has arisen that may compromise the security and integrity of the My Health Record system. As such, the healthcare provider organisation would be required to comply with s 75 of the My Health Records Act when reporting and responding to the potential breach.

# What about data breaches not covered by the My Health Records Act?

There are some situations in which a breach does not have to be reported under the My Health Records Act. This could include, for example, where a data breach has not occurred through the use of the My Health Records system but rather through the use of a registered healthcare provider organisation's, RRO's, RPO's or registered contracted service provider's local records (for example, information that is contained in, or has been downloaded from the My Health Record system into, a healthcare provider's clinical system). A data breach does not have to be reported under the My Health Records Act if it does not involve a reporting entity. As noted above, the breach notification provisions in the My Health Records Act only apply if a reporting entity is involved or may be involved in the type of contravention, event or circumstances detailed in s 75 of the My Health Records Act. Involvement in a notifiable data breach may be:

- the result of the actions of a member of staff (or a contractor) of the entity
- in connection with the entity's access to or use of the My Health Record system
- in relation to the entity's IT or other systems which directly feed into or interoperate with the My Health Record system.

## The broader Notifiable Data Breaches (NDB) scheme

From 22 February 2018, a broader Notifiable Data Breaches (NDB) scheme will apply in Australia. It will apply to organisations covered by the Privacy Act, including most Australian Government agencies, some private sector and not-for-profit organisations, and all private health service providers. It would generally not apply to state or territory authorities, or a prescribed instrumentality of a state.

The NDB scheme requires organisations covered by the scheme to notify particular individuals and the OAIC about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access or unauthorised disclosure of personal information, or a loss of personal information, that the organisation holds
2. this is likely to result in serious harm to one or more individuals, and
3. the organisation has not been able to prevent the likely risk of serious harm with remedial action.

When an entity experiences an eligible data breach, it must provide a statement to the Commissioner, and notify individuals at risk of serious harm of the contents of the statement. If it is not practicable to notify individuals at risk of serious harm, an entity must publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm. The notification must include the organisation's identity and contact details, describe the eligible data breach and the kind of information concerned and also set out recommendations about the steps individuals should take in response to the data breach.

**Example**
An eligible data breach under the NDB scheme could include where a USB device containing a healthcare provider's local patient records is lost or stolen. This would not be a breach under the My Health Records Act, as the breach does not concern the My Health Record system, but may amount to an eligible data breach under the NDB scheme.

Further information about the NDB scheme is available on the OAIC website.

# Part 2: Reporting requirements for registered healthcare provider organisations, RROs, RPOs and registered contracted service providers

## What should you do when you become aware of a notifiable data breach?

Reporting entities must report a notifiable data breach as soon as practicable after becoming aware of the breach. However, reporting the breach should not be at the expense of initial efforts to contain it. The OAIC recognises that some information about the breach may not be available when an initial report is made. This should not delay reporting, as further information can be provided when it becomes available.

Further, any steps taken by the entity to rectify or contain the breach do not relieve the entity of its reporting obligations.

If there is uncertainty about whether the breach is notifiable under the My Health Records Act, the OAIC recommends reporting the breach. The OAIC's response to the breach will not necessarily be different if the breach reported is voluntary or mandatory, but reporting the breach will mean that entities can be confident that they are meeting their obligations under the My Health Records Act.

## When should you ask the System Operator to notify affected healthcare recipients?

As set out above, most registered healthcare provider organisations, RROs, RPOs and registered contracted service providers must report notifiable data breaches to both the OAIC and the System Operator.[7] These entities cannot notify affected healthcare recipients directly about the breach, but must ask the System Operator to do this on their behalf where:

- the entity becomes aware of a ***confirmed*** notifiable data breach in which they are involved, or
- the entity becomes aware of a ***potential*** notifiable data breach in which they are involved and
    - there is a reasonable likelihood that the data breach occurred, and
    - the effects might be serious for at least one healthcare recipient.

Asking the System Operator to notify affected healthcare recipients is a separate step to reporting the notifiable data breach and, where this is required, must be carried out as soon as practicable after becoming aware of the breach.

[7] As noted above, state and territory entities are only required to report data breaches to the System Operator.

## How should you report a notifiable data breach?

Reporting of notifiable data breaches should preferably be in writing, although notification by other means will also meet the requirements set out in the My Health Records Act. In urgent cases, the OAIC encourages preliminary notification followed by more detailed notification.

The OAIC plans to have a notification form available on its website. Once available we will prefer you to use that form.

If you are not using the data breach notification form (once available), you can notify the OAIC of breaches using the following contact details:

| | |
|---|---|
| **Telephone:** | 1300 363 992 |
| **Email:** | enquiries@oaic.gov.au |
| **Post:** | GPO Box 5218,<br>Sydney NSW 2001 |
| **Facsimile:** | 02 9284 9666 |

As a separate step, you must contact the System Operator by email at MyHealthRecord.Compliance@digitalhealth.gov.au to provide the same details and, if known, tell the System Operator who the affected healthcare recipients are so that, where this is required, the System Operator can notify them of the breach. See Part 3 for more information about notification of affected healthcare recipients.

If you do not use the form (once available) to notify the OAIC, you should make sure the notification you provide through other means (such as via email, hard copy correspondence or telephone) includes all of the information listed below (where applicable).

## What should you include in a breach notification?

Use of the OAIC's mandatory data breach notification form (once available) will assist you to provide the correct information to help the OAIC determine whether the steps entities are required to take under s 75 of the My Health Records Act have been followed and have adequately been met. If the OAIC considers that further details are needed about the data breach and related issues, you will be asked to provide additional information. Notifications to the OAIC and the System Operator should include the following details (where applicable):

- a description of the data breach outlining the confirmed or potential unauthorised collection, use or disclosure or threat to the security or integrity of the My Health Record system
- the type of personal information involved
- how many healthcare recipients were or may have been affected
- when the data breach occurred, or may have occurred
- what caused, or may have caused, the data breach
- whether the breach was inadvertent or intentional
- when and how you became aware of the breach

- whether the data breach has been contained
- what action has been taken or is being taken to mitigate the effect of the data breach and/or prevent further breaches
- whether the data breach appears to stem from a systemic issue or an isolated trigger
- any other entities involved
- whether your organisation has experienced a similar breach in the past
- any measures that were already in place to prevent the breach
- whether a data breach response plan was in place, and if it has been activated
- the name and contact details of an appropriate person within your organisation
- any other relevant factors.

The appropriate amount of detail to include in the notification will depend on the nature of the breach. Where an entity identifies that a breach is minor, isolated or contained, it may be appropriate for the entity to focus on providing a brief overview of the breach, the consequences (if any) of the breach and the follow-up actions taken by the entity. In contrast, where an entity identifies that a breach is serious, widespread or ongoing (for example, because the breach affects or potentially affects a large number of healthcare recipients, the effect of the breach is or is likely to be significant for the healthcare recipients, or the factors leading to the breach have not yet been identified or addressed), more detailed information will be required in the notification.

Do not include information about the identities of affected healthcare recipients in your notification to the OAIC. You should provide this information separately to the System Operator as part of the process set out in Part 2 of this guide.

## What happens when you report a notifiable data breach to the OAIC?

The OAIC will assess each notification it receives to determine:

- if it contains sufficient information about the breach
- if appropriate action has been or is being taken
- if further action is warranted.

The OAIC will then consider whether the circumstances warrant opening an investigation (see Part 5), or whether to provide advice about further steps the entity could take in relation to the breach.

## What happens if a notifiable data breach is not reported?

The Information Commissioner has the power to seek a civil penalty if a registered healthcare provider organisation, RRO, RPO or registered contracted service provide fails to report a notifiable data breach. This includes where a registered healthcare provider organisation, RRO, RPO or registered contracted service provider:

- fails to report a notifiable data breach as soon as practicable after becoming aware of it

- reports a notifiable data breach to only the System Operator but not to the OAIC, or vice versa.[8]

The civil penalty is an amount up to 100 penalty units. [9]

The Information Commissioner has published the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*, which is a legislative instrument outlining the Commissioner's approach to the use of enforcement powers under the My Health Records Act and related legislation.

[8] As noted above, state and territory entities are only required to report data breaches to the System Operator.

[9] See s 75 of the My Health Records Act.

# Part 3: The System Operator's requirements for notifiable data breaches

## Notifying the OAIC about breaches the System Operator is involved in

The System Operator must report all notifiable data breaches to the OAIC if the notifiable data breach:

- directly involved the System Operator
- may have involved he System Operator or
- may involve the System Operator.

The System Operator should apply the same guidance on notification obligations, and follow the same reporting process and requirements, that are set out above in the section for registered healthcare provider organisations, RROs, RPOs and registered contracted service provides.

There is no penalty if the System Operator fails to report a notifiable data breach to the OAIC. However, the OAIC may investigate if it has reason to suspect that a notifiable data breach has not been reported.[10]

## Notifying healthcare recipients and the general public about notifiable data breaches

Section 75 of the My Health Records Act sets out the circumstances where healthcare recipients are notified of a data breach. Only the System Operator is responsible for notifying healthcare recipients of a breach.

The System Operator must notify all affected or potentially affected healthcare recipients if:

- the System operator becomes aware of a ***confirmed*** data breach that involves itself
- if the Systems Operator becomes aware of a ***potential*** data breach that involves itself and
    - if there is a reasonable likelihood that the data breach occurred, and
    - the effects might be serious for at least one healthcare recipient.

The System Operator must also notify all affected healthcare recipients if:

- a registered healthcare provider organisation, RRO, RPO or a registered contracted service provider asks the System Operator to notify affected healthcare recipients of a ***confirmed*** data breach
- a registered healthcare provider organisation, RRO, RPO or a registered contracted service provider asks the System Operator to inform healthcare recipients that would be affected of a ***potential*** data breach

[10] See s 73(4) of the *My Health Records* Act and Part V of the Privacy Act.

- if there is a reasonable likelihood that the data breach occurred, and
- the effects might be serious for at least one healthcare recipient.

If a significant number of healthcare recipients are affected by a ***confirmed*** breach (rather than a ***potential*** breach), the System Operator must notify the general public, in addition to notifying all the affected healthcare recipients individually.

Where notification is required, the System Operator should notify healthcare recipients as soon as practicable after becoming aware of the breach, to help healthcare recipients mitigate the effects of the breach.

For notification to affected healthcare recipients to be effective, the information in the notification should assist them to reduce or prevent any harm that could be caused by the breach. The information to be included, and the method of notification, will depend on what the System Operator considers practicable under the circumstances of the particular breach. However, as a guide, the types of information that could be included and recommended notification methods are outlined in *Data breach notification — A guide to handling personal information security breaches*.

# Part 4: Responding to a notifiable data breach

The My Health Records Act requires reporting entities to take certain steps as soon as practicable after becoming aware of a notifiable data breach (in addition to reporting the breach).[11] The steps are slightly different if the data breach has occurred compared to if the data breach may have occurred (and the difference is noted below).

Entities that fail to carry out these steps will not be subject to a civil penalty, but they may be subject to an investigation under the My Health Records Act or the Privacy Act. Depending on the circumstances, they may also have their registration under the My Health Records system varied, cancelled or suspended by the System Operator.[12]

Registered healthcare provider organisations, RROs, RPOs and registered contracted service providers should undertake steps 1 and 2, as detailed below, either simultaneously or in quick succession and ask the System Operator to undertake step 3 at the same time or as soon as possible. The System Operator should endeavour to undertake steps 1, 2 and 3 either simultaneously or in quick succession.

In addition, the reporting entity should have an existing data breach response plan that reflects and implements these steps in the context of that specific entity. A data breach response plan is a document which sets out the framework for an entity's response to a data breach. For example, a plan could set out contact details for appropriate staff to be notified, clarify the roles and responsibilities of staff, and document processes which will assist the agency or organisation to contain breaches, coordinate investigations and breach notifications, and cooperate with external investigations. A data breach response plan that includes procedures and clear lines of authority may assist in ensuring a quick response to breaches, and in providing greater potential for containing breaches and mitigating harm.[13]

[11] See s 75(5) and (6) of the My Health Records Act.

[12] See s 51(3) of the My Health Records Act.

[13] Further information on data breach response plans is available in the OAIC's *Guide to securing personal information* and *Data breach notification — A guide to handling personal information security breaches*. For an example of a data breach response plan, see the OAIC's Data breach response plan.

## Step 1: Contain the breach and undertake a preliminary assessment

| | |
|---|---|
| **Contain the breach** | Take whatever steps are appropriate to immediately contain the breach.<br><br>This could include, for example, stopping the unauthorised practice or shutting down the repository or portal that was breached, if appropriate. If it is not practical to shut down the repository or portal, or if this would result in loss of evidence, then it may be necessary to revoke or change computer access privileges or address weaknesses in physical or electronic security.<br><br>Assess whether steps can be taken to mitigate the harm healthcare recipients may suffer as a result of a breach. |
| **Undertake a preliminary assessment of the causes**<br><br>(This is required in case of a breach that has occurred. It is advisable as best practice where a breach may have occurred) | Quickly appoint someone to lead the initial assessment (if you have a data breach response plan in place, you may already have identified a breach response team). This person should be suitably experienced and have sufficient authority to conduct the initial investigation, gather any necessary information and make initial recommendations. A more detailed evaluation may subsequently be required.<br><br>The preliminary assessment should consider the following questions:<br><br>• what personal information was or may have been involved in the breach?<br><br>• what was the cause of the breach?<br><br>• what is the extent of the breach?<br><br>• what harm or humiliation to healthcare recipients could be caused by the breach? |
| **Ensure that all relevant parties are notified as soon as practicable** | Determine who needs to be made aware of the breach (internally and externally) at this preliminary stage.<br><br>As required under s 75(2) of the My Health Records Act, the OAIC and/or System Operator must be notified as soon as practicable.<br><br>Healthcare recipients affected by a ***confirmed*** notifiable data breach will also need to be notified by the System Operator.<br><br>Healthcare recipients that would be affected by a ***potential*** notifiable data breach would also need to be notified if:<br><br>• there is a reasonable likelihood that the data breach occurred, and<br><br>• the effects might be serious for at least one healthcare recipient. |

| | |
|---|---|
| | (these are mandatory requirements under the My Health Records Act).<br><br>Escalate the matter internally as appropriate. Inform the person or group within the entity responsible for privacy compliance and/or inform relevant internal investigation units. |
| **Other matters** | Ensure appropriate records of the data breach are maintained, including the steps taken to rectify the situation and the decisions made. |

## Step 2: Evaluate any risks that may be related to or arise from the breach

| **(a) Consider the type of personal information involved** | |
|---|---|
| **Considerations** | **Comments and examples** |
| Does the type of personal information that has been compromised create a greater risk of harm? | Some information is more likely to cause a healthcare recipient harm if it is compromised, whether that harm is physical, financial or psychological.<br><br>For example, an inappropriate disclosure of a healthcare recipient's health information may pose a greater risk of harm or humiliation to a healthcare recipient than, for instance, their name or address in isolation.<br><br>A combination of personal information typically creates a greater risk of harm than a single piece of personal information. If there have been other breaches, the combined information disclosed could increase the risk. |
| Who is affected by the breach? | Does the breach affect individual healthcare recipients, a large number of healthcare recipients, contractors, service providers, or other entities? |
| **(b) Determine the context of the breach** | |
| **Considerations** | **Comments and examples** |
| What is the context of the personal information involved?<br><br>What parties have gained unauthorised access to the affected information? | The sensitivity of personal information also depends on the context. For example, disclosing information to others known to the healthcare recipient is more likely to cause humiliation. As outlined above, some types of personal and health information are likely to be more sensitive than others. |

| | |
|---|---|
| How could the personal information be used? | Could the information be used for fraudulent or other harmful purposes, such as to cause significant embarrassment to the affected healthcare recipient?<br><br>Could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the healthcare recipient? |
| **(c) Establish the cause and extent of the breach** | |
| **Considerations** | **Comments and examples** |
| Is there a risk of ongoing breaches or further exposure of the information? | What was the extent of the unauthorised collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online? |
| Is the personal information adequately encrypted, de-identified or otherwise not easily accessible? | Is the information rendered unreadable by security measures that protect the stored information? Is the information displayed or stored in such a way that it cannot be used if breached? |
| What was the source of the breach? | For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does the information seem to have been lost or misplaced?<br><br>The risk of harm to the healthcare recipient may be less where the breach is unintentional or accidental, rather than intentional or malicious. |
| What steps have already been taken to mitigate the harm? | Has the breach been contained? Has the full extent of the breach been assessed? Are further steps required? |
| Is this a systemic problem or an isolated incident? | When checking the source of the breach, it is important to check whether any similar breaches have occurred in the past, or could occur in future if changes are not made. Sometimes, a breach can signal a deeper problem. This may also reveal that more information has been affected than initially thought, potentially heightening the risk. |

| | |
|---|---|
| How many healthcare recipients are affected by the breach? | If the breach is a result of a systemic problem, there may be more healthcare recipients affected than first anticipated.<br><br>Even where the breach involves accidental and unintentional misuse of information, if the breach affects many healthcare recipients, this may create greater risks that the information will be misused. The entity's response should be proportionate.<br><br>While the number of affected healthcare recipients can help gauge the severity of the breach, it is important to remember that even a breach involving the personal information of only one or two healthcare recipients can be serious, depending on the information involved. |
| **(d) Assess the risk of harm to the affected healthcare recipients** | |
| **Considerations** | **Comments and examples** |
| Who is the recipient of the information? | Is there likely to be any relationship between the unauthorised recipients of the information and the affected healthcare recipients?<br><br>For example, was the disclosure to an unknown party or to a person with whom the healthcare recipients has a difficult relationship? Or was the recipient a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it (for instance, a former authorised representative bound by professional duties of confidentialities or ethical standards)? |
| What harm to healthcare recipients could result from the breach? | Examples include:<br><br>• identity theft<br><br>• threat to physical safety<br><br>• threat to emotional wellbeing<br><br>• loss of business or employment opportunities, or other financial harm<br><br>• humiliation or damage to reputation or relationships<br><br>• discrimination, bullying or marginalisation. |

| (e) Assess the risk of other harms | |
|---|---|
| **Considerations** | **Comments and examples** |
| Other possible harms, including to the entity that suffered the breach | Examples include:<br>• loss of public trust in the entity<br>• loss of public trust in the My Health Record system<br>• reputational damage<br>• loss of assets (for example, stolen computers or storage devices)<br>• regulatory penalties<br>• legal liability. |

## Step 3: Notification

| | |
|---|---|
| **When to notify** | Notification must be made as soon as practicable after becoming aware of the data breach. |
| **Who should notify healthcare recipients?** | Only the System Operator is responsible for notifying affected or potentially affected healthcare recipients about notifiable data breaches. |
| **Who should be notified?** | The **System Operator** must notify the OAIC as soon as practicable.<br>**State and territory reporting entities** must report breaches to the System Operator.<br>**All other reporting entities** must notify both the OAIC and the System Operator.[14] |
| **When should the systems operator notify healthcare recipients?** | Healthcare recipients affected by a ***confirmed*** notifiable data breach will also need to be notified.<br>Healthcare recipients that would be affected by a ***potential*** notifiable data breach also need to be notified if<br>• there is a reasonable likelihood that the data breach occurred, and<br>• the effects might be serious for at least one healthcare recipient. |

[14] As noted above, state and territory entities are only required to report data breaches to the System Operator.

| | |
|---|---|
| **When should the Systems operator notify the general public?** | Where a significant number of healthcare recipients are affected by a confirmed breach (rather than a potential breach). |

## Step 4: Take steps to prevent or mitigate the effects of further breaches

Good privacy practice is not just important for ensuring compliance with the requirements of the My Health Records Act and Privacy Act. If an entity mishandles the personal information of its clients or customers, this can cause loss of trust and considerable harm to the entity's reputation. Additionally, if personal information that is essential to an entity's activities is lost or altered, this can have a serious impact on its capacity to perform its functions or activities.

With this in mind, after assessing the causes of the breach and any associated risks, the reporting entity should set up a plan of action to prevent further breaches, as well as a data breach response plan to respond to future breaches, or review existing plans. Planning should include actions that are proportionate to the significance of the breach, and take into account whether it was a systemic breach or an isolated event.

Under the My Health Records Act, reporting entities are required to undertake this step if they are involved in a breach that has occurred. For suggested preparations for responding to a data breach and tips for preventing future breaches see *Data breach notification — A guide to handling personal information security breaches*.

For more general information on steps and strategies to take protect personal information see the OAIC's *Guide to securing personal information*. The Guide to securing personal information outlines appropriate security safeguards for personal information such as the use of privacy enhancing technologies, conducting privacy impact assessments, policy development, complaint handling, contract management and staff training.

# Part 5: Regulation of notifiable data breach reporting

## Enforcement

The OAIC has the role of receiving data breach notifications from reporting entities, and can seek a civil penalty if a registered healthcare provider organisation, RRO, RPO or registered contracted service provider does not report a notifiable data breach. The functions and enforcement powers available under the My Health Records Act give the Information Commissioner the ability to:

- use existing Privacy Act investigative and enforcement mechanisms, including Commissioner initiated investigations, conciliation of complaints, formal determinations and audits/assessments[15]
- accept enforceable written undertakings from an entity requiring them to take or refrain from taking specified action(s) to comply with the My Health Records Act. These may be enforced by the courts[16]
- seek an injunction (order) from the courts to prohibit or require particular conduct[17]
- seek a civil penalty from the courts.[18]

As mentioned above, the Information Commissioner has published the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* which outline the Commissioner's approach to the use of enforcement powers under the My Health Records Act and related legislation.

## Investigations in relation to notifiable data breaches

The OAIC may conduct investigations and take enforcement action relating to notifiable data breaches in relation to:

- a reporting entity's compliance with its notifiable data breach reporting obligations (described in this guide)
- a possible data breach by a reporting entity.[19]

## Investigating notifiable data breach reporting obligations

If it appears that an entity may not have complied with its notifiable data breach reporting obligations, the OAIC may open a Commissioner initiated investigation. The OAIC may be alerted to this possibility by, for example:

- media coverage

[15] See Part V of the Privacy Act.

[16] See s 80 of the My Health Records Act and Part 6 of the *Regulatory Powers (Standard Provisions) Act 2014*.

[17] See s 81 of the My Health Records Act and Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014*.

[18] See s 79 of the My Health Records Act and Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*.

[19] See s 73(4) of the My Health Records Act and Part V of the Privacy Act.

- anonymous tip offs
- individual complaints where no corresponding notifiable data breach report has been received or
- notifiable data breaches that are reported to the System Operator but not the OAIC (or vice versa).

Even if the OAIC does not investigate a possible breach (see below), it may still investigate the reporting entity's compliance with its data breach reporting obligations.

## Investigating possible notifiable data breaches

If the OAIC receives complaints from affected healthcare recipients about a possible data breach, it will consider whether to open an investigation, but in some situations it will not investigate. For example, it will generally not investigate where:

- the complainant has not complained to the entity first and given it the opportunity to respond (generally within 30 days of the complaint being made)
- the entity has adequately dealt with the matter
- the complaint was made more than 12 months after the complainant became aware of the matter
- the complaint is frivolous, vexatious, misconceived or lacking in substance.

Where the healthcare recipient has been unable to resolve the matter with the reporting entity directly, the OAIC may attempt to resolve the matter by conciliation between the parties. Where appropriate, the Commissioner may make determinations requiring certain remedies. Determinations can be enforced by the Federal Court or Federal Circuit Court of Australia.[20]

If the OAIC receives a notifiable data breach report but receives no complaint from the affected healthcare recipient(s), it will assess whether a Commissioner initiated investigation into the breach is warranted. The criteria the OAIC may use to open a Commissioner initiated investigation include:

- the significance of the breach and sensitivity of the personal information involved
- whether a large number of healthcare recipients have been, or are likely to be affected, and the possible consequences for those healthcare recipients
- the likelihood that the breach is due to systemic issues within the reporting entity
- how the reporting entity has responded to the data breach, including whether the entity has followed the requirements of the My Health Records Act
- the systems and processes the reporting entity had in place before the breach occurred
- whether the breach has been adequately dealt with in the OAIC's opinion
- the progress of the entity's own investigation into the matter. If the OAIC receives a notifiable data breach report while the entity's internal investigation is underway, the OAIC may wait until the internal investigation is complete

[20] These investigative and enforcement powers and functions are granted to the Commissioner under the Privacy Act.

- whether another body, such as the police, is investigating the breach.

This is not an exhaustive list and the Information Commissioner may take any other relevant matters into account when deciding whether to open a Commissioner initiated investigation.[21]

[21] Other factors that may be considered in determining whether to open a Commissioner initiated investigation are outlined in the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*.

# Appendix A: Data breach response

## When should you follow this data breach response plan?

1. A My Health Record Act data breach occurs, AND

   (see above '*Under the My Health Record system, what is a data breach*?')

2. You are a reporting entity, AND

   (see above '*Who is required to report a data breach?*')

3. You become aware that you may be involved in the breach.

   (see above '*When are they required to report the breach?*')

## What should you do?

**Step 1: *Contain the breach and undertake a preliminary assessment***

**Step 2: *Evaluate any risks that may be related to or arise from the breach***

**Step 3: *Notify:***

| System Operator | State and territory reporting entities | All other reporting entities |
|---|---|---|
| → the OAIC<br>→ in some circumstances, healthcare recipients and/or the general public | → System Operator | → the System Operator<br>→ the OAIC |
| (see above '*Notifying healthcare recipients and the general public about notifiable data breaches')* | | |

**Step 4: *Take steps to prevent or mitigate the effects of further breaches***

## What if the privacy breach does not involve the My Health Records System?

Entities should follow the OAIC's *Data breach notification — A guide to handling personal information security breaches* when considering reporting data breaches voluntarily.

(See above '*What about data breaches not covered by the My Health Records Act*')

# Appendix B: Compliance checklist

This checklist is only a summary of reporting entities' key data breach obligations under s 75 of the My Health Records Act. Penalties, including civil penalties, may apply for non-compliance with data breach notification obligations.

## For the System Operator, registered healthcare provider organisations, RROs, RPOs and registered contracted service providers:

- ☐ We have taken steps to contain the breach (as far as is reasonably practicable).
- ☐ We have undertaken a preliminary assessment of the causes of the breach.
- ☐ We have evaluated any risks that may be related to or arise from the breach.
- ☐ We have taken steps to prevent or mitigate the effects of further breaches.

## For registered healthcare provider organisations, RROs, RPOs and registered contracted service providers who are a State/Territory authority:

- ☐ We have reported the breach to the System Operator.
- ☐ Where required, we have told the System Operator which healthcare recipients were affected or potentially affected and asked the System Operator to notify those healthcare recipients of the breach.

## For other registered healthcare provider organisations, RROs, RPOs and registered contracted service providers:

- ☐ We have reported the breach to both the OAIC and the System Operator.
- ☐ Where required, we have told the System Operator which healthcare recipients were affected or potentially affected and asked the System Operator to notify those healthcare recipients of the breach.

## For the System Operator:

- ☐ I have reported the breach to the OAIC.
- ☐ Where required, I have notified the affected or potentially affected healthcare recipients (and the general public if a significant number of healthcare recipients are affected).

# Appendix C: Data breach notification, legislative framework and regulatory approach

## The breach notification provisions in the My Health Records Act

The breach notification provisions are outlined in s 75 of the My Health Records Act.[22] In summary, s 75 sets out:

- which entities have mandatory notification obligations
- what contraventions, events or circumstances constitute a notifiable data breach under the My Health Records Act
- when and to whom the System Operator, a registered healthcare provider organisation, RRO, RPO or registered contracted service provider should report a notifiable data breach
- the other actions these entities must take in response to such a breach.

Sections 75(2) and 79 of the My Health Records Act establish civil penalties for the failure of registered healthcare provider organisation, RRO, RPO and registered contracted service provider to report a notifiable data breach to the System Operator and/or OAIC as soon as practicable after becoming aware of the breach.

## Entities to which the breach provisions apply

Sections 75(1) provides that the breach notification provisions apply to an entity if the entity is, or has at any time been, the System Operator, a registered healthcare provider organisation, an RRO, an RPO or a registered contracted service provider and the entity becomes aware of a notifiable data breach.

## Types of data breaches that must be reported

Under s 75(1), a notifiable data breach occurs if the System Operator, a registered healthcare provider organisation, RRO, RPO or registered contracted service provider becomes aware that:

- a person has, or may have, contravened the My Health Records Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record or
- an event has, or may have, occurred or circumstances have arisen (regardless of whether or not involving a contravention of the My Health Records Act) that compromise, may compromise, has compromised or may have compromised, the security or integrity of the My Health Record system

AND the contravention, event or circumstances directly involved, may have involved or may involve the System Operator, a registered healthcare provider organisation, RRO, RPO or registered contracted service provider.

[22] Section 75 of the *My Health Records* Act is available at www.comlaw.gov.au/Series/C2012A00063.

## When and to whom reporting entities must report a breach

Section 75(2) provides that a registered healthcare provider organisation, RRO, RPO or a registered contracted service provider must notify both the System Operator and the Information Commissioner as soon as practicable after becoming aware of the a notifiable data breach.

Section 75(3) states that the System Operator must notify the Information Commissioner as soon as practicable after becoming aware of a notifiable data breach.

## Other actions that must be taken to deal with a breach

Section 75(5) and (6) set out the steps that reporting entities must take depending on whether the contravention, event or circumstance:

- may have occurred or arisen or
- has been confirmed as having occurred or arisen.

Where a breach may have occurred or arisen, s 75(5) states that a reporting entity must, as soon as practicable after becoming aware that the contravention, event or circumstances may have occurred or arisen, do the following things:

- so far as is reasonably practicable, contain the contravention, event or circumstances
- evaluate any risks that may be related to or arise out of the contravention, event or circumstances
- if there is a reasonable likelihood that the contravention, event or circumstances has occurred or arisen and the effects of the contravention, event or circumstances might be serious for at least one healthcare recipient:
    - if the entity is not the System Operator – ask the System Operator to notify all healthcare recipients that would be affected or
    - if the entity is the System Operator – notify all healthcare recipients that would be affected.

Where there is a confirmed breach, s 75(6) states that a reporting entity must, as soon as practicable after becoming aware that the contravention or event has occurred or the circumstances have arisen, do the following things:

- so far as is reasonably practicable, contain the contravention, event or circumstances and undertake a preliminary assessment of the causes
- evaluate any risks that may be related to or arise out of the contravention, event or circumstances
- if the entity is the System Operator
    - notify all affected healthcare recipients and
    - if a significant number of healthcare recipients are affected, notify the general public
- if the entity is not the System Operator – ask the System Operator
    - to notify all affected healthcare recipients and
    - if a significant number of healthcare recipients are affected, notify the general public

- take steps to prevent or mitigate the effects of further contraventions, events or circumstances that compromise the security or integrity of the My Health Record system.

Part 4 of the guide provides more information on how reporting entities can meet their obligations under s 75(4).

## The My Health Records Act and the Privacy Act

The handling of a healthcare recipient's health information in the My Health Record system may be covered by both the Privacy Act and the My Health Records Act. The Information Commissioner has enforcement powers under both Acts and may choose to investigate a notifiable data breach under either Act depending on the circumstances.[23] For more information about the role of the Information Commissioner in regulating the privacy aspects of the My Health Record system, see below and Part 5.

## The Privacy Act

The Privacy Act regulates the handling of personal information by the System Operator and all private sector healthcare provider organisations. More generally, the Privacy Act applies to private sector organisations (not including small businesses) and Australian government, and Norfolk Island agencies.[24]

The Privacy Act establishes a number of privacy principles that regulate the collection, use, disclosure and secure storage of personal information. A breach of a privacy principle by an entity is an 'interference with the privacy of an individual' for the purposes of the Privacy Act. Under the Privacy Act, the OAIC can investigate complaints about alleged interferences with the privacy of an individual.

## The interaction of the Privacy Act and the My Health Records Act

Parts 4 and 5 of the My Health Records Act contain provisions that regulate the collection, use and disclosure of personal information by participants. This creates some overlap between the My Health Records Act and the privacy principles in the Privacy Act.

There are two main ways that the Privacy Act and My Health Records Act manage this overlap.

First, certain privacy principles in the Privacy Act contain exceptions to allow collection, use or disclosure of personal information where it is required or authorised by law. For example, disclosure of personal information that is otherwise prohibited under the Privacy Act is allowable if is required by the My Health Records Act. Other privacy principles in the Privacy Act, such as those relating to collection notices, data security and data accuracy, continue to apply.

Second, the My Health Records Act states that any breach of that Act in connection with health information included in a healthcare recipient's My Health Record is an 'interference with privacy of the healthcare recipient' for the purposes of the Privacy Act. This triggers the Information Commissioner's

[23] For more information on how the Information Commissioner will exercise enforcement powers in relation to the My Health Record system, see the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2013*.

[24] The *Information Privacy Act 2014 (ACT)* regulates how personal information is handled by ACT public sector agencies. However, under an arrangement between the ACT Government and the Australian Government, the Australian Information Commissioner is exercising some of the functions of the ACT Information Privacy Commissioner. These responsibilities include handling privacy complaints against, and receiving data breach notifications from, ACT public sector agencies

enforcement and investigation powers under the Privacy Act. The My Health Records Act contains additional enforcement powers that recognise and aim to protect the sensitivity of health information.

Whether the My Health Records Act applies to a particular act or practice will depend on whether the act or practice was related to the My Health Record system. For example, general handling of health information that does not use the My Health Record system, such as within an entity's own IT system or paper records, will not be covered by the My Health Records Act, but is likely to be covered by the Privacy Act (because the entity will be handling personal information).

## Information security provisions in the Privacy Act and the My Health Records Act

Reporting entities should take care to comply with their information security obligations under the Privacy Act. Entities that have complied with their security obligations will be less likely to experience a data breach. If a breach does occur, the Information Commissioner may ask the entity to demonstrate how it met its Privacy Act obligations.

Security principles under the Privacy Act generally require organisations (such as some RROs and RPOs that are private sector organisations) and agencies (such as the System Operator) to take reasonable steps to protect the information they hold from misuse and loss and from unauthorised access, modification or disclosure.

These security principles operate in addition to any specific security provisions contained in the My Health Records Act and subordinate legislation. Complying with the provisions of the My Health Records Act may help an entity meet its security obligations under the Privacy Act, however the entity must also take all 'reasonable steps' to secure the information, as required by the Privacy Act. More information about how to comply with security principles in the Privacy Act can be found in the OAIC's *Guide to securing personal information*.

## Role of the Information Commissioner under the My Health Record system

The OAIC is an independent statutory agency headed by the Information Commissioner. The OAIC regulates the Privacy Act and *Freedom of Information Act 1982* (Cth), and works to advance the development of consistent, workable information policy across all Australian Government agencies.

The OAIC regulates the handling of personal information in the My Health Record system by individuals, Australian government agencies, private sector organisations and some state and territory agencies (in particular circumstances). The OAIC has been given a range of functions and powers to carry out its regulatory role in the My Health Record system.

The OAIC's functions and powers in relation to notifiable data breaches include:

- accepting reports about notifiable data breaches
- providing advice to reporting entities
- conducting investigations to assess reporting entities' compliance with their obligations under the My Health Records Act
- investigating reported breaches

- taking enforcement action, where the circumstances warrant it.

The regulatory section of this guide (see Regulation of notifiable data breach reporting) sets out the circumstances in which the OAIC will conduct an investigation about a notifiable data breach and the OAIC's enforcement powers. What happens when you report a notifiable data breach to the OAIC outlines the actions the OAIC may take when it receives a report, including its role in providing advice to reporting entities about complying with their obligations under the Act.

For more information about the regulation of data breach notification, see Part 5.

## Role of the System Operator

The System Operator manages and operates core aspects of the My Health Record system. The functions of the System Operator are set out in s 15 of the My Health Records Act and include:

- registration of healthcare recipients, healthcare providers, repository operators, portal operators and contracted service providers
- maintaining the National Repositories Service, system access controls, a clinical document index service and audit service
- establishing a complaint handling framework
- educating participants in the system.

The System Operator also receives mandatory data breach notifications from registered healthcare provider organisations, RROs, RPOs and registered contracted service providers. It will liaise with the OAIC and may investigate breaches, take corrective actions and help the reporting entity to mitigate any loss or damage that may result from the breach. The System Operator is required to notify affected, or in some circumstances, potentially affected healthcare recipients of a breach and, where a significant number of healthcare recipients are affected, the general public. The System Operator cannot seek civil penalty orders if a reporting entity fails to report a notifiable data breach to it, but it may cancel, suspend or vary the registration of a registered healthcare provider organisation, RRO, RPO or registered contracted service provider.

If the System Operator has or may have been involved in a notifiable data breach, it must report the breach to the Information Commissioner. For more information about the System Operator's breach notification obligations, see Part 3.

# Glossary

**Healthcare recipient** has the meaning set out in s 5 of the My Health Records Act and means an individual who has received, receives or may receive healthcare.

**Data breach** means, in general terms, when personal information is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse. This term is not defined in the My Health Records Act, however it has entered into common usage in Australia and in various other jurisdictions. 'Notifiable data breach' is used in this guide to describe the types of data breaches that must be notified to the appropriate regulator under the My Health Records Act (see definition below).

**Entity** has the meaning set out in s 5 of the My Health Records Act and means:

(a) a person or

(b) a partnership or

(c) any other unincorporated association or body or

(d) a trust or

(e) a part of an entity (under a previous application of this definition).

In this guide, 'reporting entity' refers to specific kinds of entities (see definition below).

**Health information** has the meaning set out in s 6(1) of the Privacy Act.

**Healthcare provider organisation** has the meaning set out in s 5 of the My Health Records Act and means an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).

Because of paragraph (e) of the definition of ***entity***, a healthcare provider organisation could be a part of an entity.

A healthcare provider organisation could also be an individual, such as a sole practitioner.

The **National Repositories Service** has the meaning set out in s 5 of the My Health Records Act and is a data repository that stores key records that form part of a registered healthcare recipient's My Health Records, including a healthcare recipient's shared health summary.

**Notifiable data breach** is used in this guide to refer to the types of data breaches described in s 75(1) of the My Health Records Act. For more information, see Part 1.

**OAIC** means the Office of the Australian Information Commissioner.

**My Health Records Act** means the *My Health Records Act 2012* (Cth).[25]

**My Health Record system** has the meaning set out in s 5 of the My Health Records Act and means a system:

(a) that is for:

(i) the collection, use and disclosure of information from many sources using telecommunications services and by other means, and the holding of that information, in

[25] www.comlaw.gov.au/Current/C2013C00295

accordance with the healthcare recipient's wishes or in circumstances specified in this Act and

(ii) the assembly of that information using telecommunications services and by other means so far as it is relevant to a particular healthcare recipient, so that it can be made available, in accordance with the healthcare recipient's wishes or in circumstances specified in this Act, to facilitate the provision of healthcare to the healthcare recipient or for purposes specified in this Act and

(b) that involves the performance of functions under this Act by the System Operator.

**Personal information** has the meaning as set out in s 6 of the Privacy Act:

personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not and

(b) whether the information or opinion is recorded in a material form or not.[26]

**Privacy Act** means the *Privacy Act 1988* (Cth).[27]

**Registered contracted service provider** has the meaning set out in s 5 of the My Health Records Act and means a contracted service provider that is registered under s 49 of the My Health Records Act.

**Registered healthcare provider organisation** has the meaning set out in s 5 of the My Health Records Act and means a healthcare provider organisation that is registered under s 44 of the My Health Records Act.

A **registered portal operator (RPO)** has the meaning set out in s 5 of the My Health Records Act and means a person that:

(a) is the operator of an electronic interface that facilitates access to the My Health Record system and

(b) is registered as a portal operator under s 49 of the My Health Record Act.

A **registered repository operator (RRO)** has the meaning set out in s 5 of the My Health Records Act and means a person that:

(a) holds, or can hold, records of information included in personally controlled electronic health records for the purposes of the My Health Record system and

(b) is registered as a repository operator under s 49 of the My Health Record Act.

**Reporting entity** is used in this guide to refer to the System Operator, a registered healthcare provider organisation, a registered portal operator, a registered repository operator or a registered contracted service provider.

**State or territory entity** means a state or territory authority or instrumentality. 'State or territory authority' is defined in s 6 of the Privacy Act.

[26] This definition is from the reformed Privacy Act which commenced on 12 March 2014. Before 12 March 2014, please refer directly to the Privacy Act.

[27] www.comlaw.gov.au/Current/C2013C00482

**System Operator** has the meaning set out is s 5 of the My Health Records Act. The System Operator manages and operates the core aspects of the My Health Record system. The Australian Digital Health Agency is currently the System Operator.

A **use** of health information included in a healthcare recipient's My Health Record is defined under the My Health Record Act to include:

(a) accessing the information

(b) viewing the information

(c) modifying the information and

(d) deleting the information.