DOCUMENT 1

Australian Government
Office of the Australian Information Commissioner

My Health Record Data Breach Notification Form

Who should use this form?

This form is intended for use by the My Health Record System Operator, registered repository operators, healthcare provider organisations and registered portal operators who are required to report data breaches of the My Health Record System to the Office of the Australian Information Commissioner (OAIC) under s 75 of the *My Health Records Act 2012*. Further information on data breach reporting requirements and the actions that entities need to take in response to a breach are in the OAIC's guide to *Mandatory data breach notification in the My Health Record System*.

This form is not intended for entities voluntarily reporting data breaches to the OAIC. See *Data breach notification — A guide to handling personal information security breaches* for information on how to report data breaches that are not subject to mandatory reporting requirements.

Reporting My Health Record System data breaches

The System Operator, registered repository operators, healthcare provider organisations and registered portal operators are required to report data breaches to the OAIC as soon as practicable. It is not compulsory for entities to use this form to report a My Health Record System data breach to the OAIC. However, if you do not wish to use this form, you must notify the OAIC of the details requested below (where applicable).

The OAIC recognises that not all information requested on the form will be available when you first notify the OAIC of a data breach. Any information that you are unable to provide when making the initial report should be provided as it becomes available.

If you have any questions about this form or mandatory data breach reporting requirements, please email the OAIC Enquiries Line enquiries@oaic.gov.au or call 1300 363 992. Email contact is preferred.

Submitting this form

Please send the completed form by email to enquiries@oaic.gov.au, or by fax to (02) 9284 9666.

Information on actions the OAIC may take in relation to data breaches is available in the OAIC's guide to Mandatory data breach notification in the My Health Record System.

Organisation/agency details

Name of organisation/agency: Australian Digital Health Agency

Is your organisation/agency: My Health Record System Operator

Contact officer details

Name:

Tony Kitzelmann

Title/role within the organisation/agency: **General Manager and Chief Information Security Officer, Cyber Security Centre, Core Services Systems Operations Division**

Email: **anthony.kitzelmann@digitalhealth.gov.au**

Contact phone number: **(07) 3023 8421**

Please advise the OAIC as soon as possible of any change in contact details.

Details of the breach

Please provide the following details where available/applicable. Additional pages can be attached if required.

Description of the breach, outlining the suspected unauthorized collection, use or disclosure or threat to the security or integrity of the My Health Record System:

A DHS service officer acting as a delegate of the System Operator incorrectly registered a child for a My Health Record under their own identity and also accessed the record upon completion of the process.

When did the breach occur?

27 August 2014 when the child's parent contacted the My Health Record helpline to have the child registered and the parent established as an authorized representative (parental).

What type of personal information was involved in the breach?

Only demographic information of the child. There were no other documents in the My Health Record at the time.

How many consumers were or may have been affected? *(Do not include any personal information of consumers affected by the breach.)*

One

What caused the breach? Please provide details of the preliminary assessment, and the outcomes of any further assessments as they are completed.

On completion of the registration process, service operators are not authorized or required to go beyond the My Health Record landing screen that presents when the process is completed. In this instance, the officer clicked the My Health Record button and gained entry to the record.

Was the breach inadvertent or intentional (for example, a deliberate act by an individual staff member)?

It would appear from system transactional information that the breach was inadvertent or unintentional.

When and how did your organisation/agency become aware of the breach?

Early May 2018. The registration error came to light during a random audit conducted by the National Infrastructure Operator (NIO) where a small number of instances of such incorrect registrations were discovered. Upon further examination of each of these registration, this breach was identified.

Were any other entities involved in the breach?

No

Has your organisation/agency experienced a similar breach(es) in the past?

No

For registered repository operators and registered portal operators

Have you notified the System Operator of the breach?

☐ Yes

☐ No

Under s 75 of the My Health Records Act, registered repository operators and registered portal operators are required to notify both the System Operator and the OAIC. A civil penalty may apply if an entity does not notify both the OAIC and the System Operator as soon as practicable. On receiving a data breach notification, the OAIC will liaise with the System Operator to ensure that it has also received notification of the data breach.

Have you asked the System Operator to notify the affected consumer(s) (and the general public if a significant number of consumers were affected)?

☐ Yes
☐ No

For the System Operator

Have you notified the affected consumer(s) (and the general public if a significant number of consumers were affected)?

If yes, when and how was this notification provided? If no, when and how do you intend to notify affected consumers?

The Department of Human Services will be contacting the child's parent to make them aware of the error and to correctly establish the link to the child's My Health Record to that of the parent as their authorised representative (parent).

The OAIC will contact you to discuss this notification and to seek further information if required. Please refer to the OAIC's guide to *Mandatory data breach notification in the My Health Record System* for further information on other actions that you are required to take in response to a data breach under s 75 of the My Health Records Act.

Please sign and date this form on behalf of your organisation/agency.

Signature: ..... …… Date:
Name of signatory:

DOCUMENT 2

Australian Government
Office of the Australian Information Commissioner

My Health Record Data Breach Notification Form

Who should use this form?

This form is intended for use by the My Health Record System Operator, registered repository operators, healthcare provider organisations and registered portal operators who are required to report data breaches of the My Health Record System to the Office of the Australian Information Commissioner (OAIC) under s 75 of the *My Health Records Act 2012*. Further information on data breach reporting requirements and the actions that entities need to take in response to a breach are in the OAIC's guide to *Mandatory data breach notification in the My Health Record System*.

This form is not intended for entities voluntarily reporting data breaches to the OAIC. See *Data breach notification — A guide to handling personal information security breaches* for information on how to report data breaches that are not subject to mandatory reporting requirements.

Reporting My Health Record System data breaches

The System Operator, registered repository operators, healthcare provider organisations and registered portal operators are required to report data breaches to the OAIC as soon as practicable. It is not compulsory for entities to use this form to report a My Health Record System data breach to the OAIC. However, if you do not wish to use this form, you must notify the OAIC of the details requested below (where applicable).

The OAIC recognises that not all information requested on the form will be available when you first notify the OAIC of a data breach. Any information that you are unable to provide when making the initial report should be provided as it becomes available.

If you have any questions about this form or mandatory data breach reporting requirements, please email the OAIC Enquiries Line enquiries@oaic.gov.au or call 1300 363 992. Email contact is preferred.

Submitting this form

Please send the completed form by email to enquiries@oaic.gov.au, or by fax to (02) 9284 9666.

Information on actions the OAIC may take in relation to data breaches is available in the OAIC's guide to Mandatory data breach notification in the My Health Record System.

Organisation/agency details

Name of organisation/agency: Australian Digital Health Agency

Is your organisation/agency: My Health Record System Operator

Contact officer details

Name: **Tony Kitzelmann**

Title/role within the organisation/agency: **General Manager and Chief Information Security Officer, Cyber Security Centre, Core Services Systems Operations Division**

Email: **anthony.kitzelmann@digitalhealth.gov.au**

Contact phone number: **(07) 3023 8421**

Please advise the OAIC as soon as possible of any change in contact details.

Details of the breach

Please provide the following details where available/applicable. Additional pages can be attached if required.

Description of the breach, outlining the suspected unauthorized collection, use or disclosure or threat to the security or integrity of the My Health Record System:

On 30 Oct 2017, a consumer reported that they had received a Medicare card with a child's name that was not their child. Investigations by the system operator showed that the child had previously been registered for a My Health Record with this consumer incorrectly assigned as their Authorised Representative and they had accessed the My Health Record of the child once.

When did the breach occur?

The breach occurred on 18 April 2017 when the incorrectly assigned Authorised Representative accessed the My Health Record of the child.

What type of personal information was involved in the breach?

The information involved in the breach was the demographic details of the child. The child's My Health Record did not contain any Medicare or clinical documents at the time.

How many consumers were or may have been affected? *(Do not include any personal information of consumers affected by the breach.)*

Two (one minor child and one Parental Authorised Representative (PAR)) consumers have been affected by this incident.

What caused the breach? Please provide details of the preliminary assessment, and the outcomes of any further assessments as they are completed.

The Department of Human Services processes the Medicare Newborn Child Registration form which includes an option for parents to register their newborn for a My Health Record. The form was processed incorrectly on 14 Jan 2017 whereby the child's My Health Record was linked to an unrelated individual as their authorized representative. The breach was caused by the incorrect representative accessing the record. The registration was corrected on 10 November 2017.

Was the breach inadvertent or intentional (for example, a deliberate act by an individual staff member)?

The breach occurred due to an operator error and was inadvertent.

When and how did your organisation/agency become aware of the breach?

The System Operator became aware of the breach on 30 October 2017 when the consumer contacted the My Health Record helpline.

Were any other entities involved in the breach?

Yes. The Department of Human Services who processed the Medicare Newborn Child Registration form.

Has your organisation/agency experienced a similar breach(es) in the past?

Yes

For registered repository operators and registered portal operators

Have you notified the System Operator of the breach?

☐ Yes

☐ No

Under s 75 of the My Health Records Act, registered repository operators and registered portal operators are required to notify both the System Operator and the OAIC. A civil penalty may apply if an entity does not notify both the OAIC and the System Operator as soon as

Have you asked the System Operator to notify the affected consumer(s) (and the general public if a significant number of consumers were affected)?

☐ Yes

☐ No

For the System Operator

Have you notified the affected consumer(s) (and the general public if a significant number of consumers were affected)?

Yes

If yes, when and how was this notification provided? If no, when and how do you intend to notify affected consumers?

The Department of Human Services via phone.

The OAIC will contact you to discuss this notification and to seek further information if required. Please refer to the OAIC's guide to *Mandatory data breach notification in the My Health Record System* for further information on other actions that you are required to take in response to a data breach under s 75 of the My Health Records Act.

Please sign and date this form on behalf of your organisation/agency.

s47F [redacted]

Signature: ..... Date: 12 Dec 17.

Name of signatory:

DOCUMENT 3

Australian Government

Office of the Australian Information Commissioner

My Health Record Data Breach Notification Form

Who should use this form?

This form is intended for use by the My Health Record System Operator, registered repository operators, healthcare provider organisations and registered portal operators who are required to report data breaches of the My Health Record System to the Office of the Australian Information Commissioner (OAIC) under s 75 of the *My Health Records Act 2012*. Further information on data breach reporting requirements and the actions that entities need to take in response to a breach are in the OAIC's guide to *Mandatory data breach notification in the My Health Record System*.

This form is not intended for entities voluntarily reporting data breaches to the OAIC. See *Data breach notification — A guide to handling personal information security breaches* for information on how to report data breaches that are not subject to mandatory reporting requirements.

Reporting My Health Record System data breaches

The System Operator, registered repository operators, healthcare provider organisations and registered portal operators are required to report data breaches to the OAIC as soon as practicable. It is not compulsory for entities to use this form to report a My Health Record System data breach to the OAIC. However, if you do not wish to use this form, you must notify the OAIC of the details requested below (where applicable).

The OAIC recognises that not all information requested on the form will be available when you first notify the OAIC of a data breach. Any information that you are unable to provide when making the initial report should be provided as it becomes available.

If you have any questions about this form or mandatory data breach reporting requirements, please email the OAIC Enquiries Line enquiries@oaic.gov.au or call 1300 363 992. Email contact is preferred.

Submitting this form

Please send the completed form by email to enquiries@oaic.gov.au, or by fax to (02) 9284 9666.

Information on actions the OAIC may take in relation to data breaches is available in the OAIC's guide to Mandatory data breach notification in the My Health Record System.

Organisation/agency details

Name of organisation/agency: Australian Digital Health Agency

Is your organisation/agency: My Health Record System Operator

Contact officer details

Name: **Tony Kitzelmann**

Title/role within the organisation/agency: General Manager and Chief Information Security **Officer, Cyber Security Centre, Core Services Systems Operations Division**

Email: **anthony.kitzelmann@digitalhealth.gov.au**

Contact phone number: **(07) 3023 8421**

Please advise the OAIC as soon as possible of any change in contact details.

Details of the breach

Please provide the following details where available/applicable. Additional pages can be attached if required.

Description of the breach, outlining the suspected unauthorized collection, use or disclosure or threat to the security or integrity of the My Health Record System:

An individual with access to a Medicare Online Account can access their Medicare claims history and make a claim for the Medicare rebate online. As part of its compliance program, the Department of Human Services has identified fraudulent Medicare online claiming activity. If this activity has resulted in fraudulent claims being sent to the My Health Record System, these claims are removed from the My Health Record by the Department of Human Services and reported to the OAIC. The consumer is also notified of the removal of the incorrect or inaccurate claims by the My Health Record System Operator.

Following advice from the Department of Human Services that fraudulent Medicare claiming information has been sent to a My Health Record, the System Operator reviews all transactional information relating to that record to determine if any other online activity has occurred i.e access or viewing of information contained in the record.

In this case, evidence indicates that it is probable that the My Health Record was created using the myGov account used to conduct the online Medicare fraud. As it cannot be conclusively determined that both actions were performed by a third party and not by the consumer themselves, the System Operator is notifying the OAIC of a potential data breach.

When did the breach occur?
28 March 2014.

What type of personal information was involved in the breach?
Consumer demographics (name, address, DOB, age, IHI) and Medicare information.

How many consumers were or may have been affected? *(Do not include any personal information of consumers affected by the breach.)*
One.

What caused the breach? Please provide details of the preliminary assessment, and the outcomes of any further assessments as they are completed.
The breach was potentially caused by a person other than the legitimate owner of the My Health Record creating and accessing a My Health Record.

Was the breach inadvertent or intentional (for example, a deliberate act by an individual staff member)?
The breach occurred due to a deliberate act by a person other than the legitimate consumer.

When and how did your organisation/agency become aware of the breach?
The System Operator became aware of the breach on 31 October 2017 when transactional data became available.

Were any other entities involved in the breach?
The Department of Human Services.

Has your organisation/agency experienced a similar breach(es) in the past?
Yes

For registered repository operators and registered portal operators

Have you notified the System Operator of the breach?

☐ Yes

☐ No

Under s 75 of the My Health Records Act, registered repository operators and registered portal operators are required to notify both the System Operator and the OAIC. A civil penalty may apply if an entity does not notify both the OAIC and the System Operator as soon as practicable. On receiving a data breach notification, the OAIC will liaise with the System Operator to ensure that it has also received notification of the data breach.

Have you asked the System Operator to notify the affected consumer(s) (and the general public if a significant number of consumers were affected)?

☐ Yes

☐ No

For the System Operator

Have you notified the affected consumer(s) (and the general public if a significant number of consumers were affected)?

Attempt was made to contact the consumer however the only address hold on the record has had a Medicare card returned to sender.

If yes, when and how was this notification provided? If no, when and how do you intend to notify affected consumers?

The Department of Human Services via phone.

The OAIC will contact you to discuss this notification and to seek further information if required. Please refer to the OAIC's guide to *Mandatory data breach notification in the My Health Record System* for further information on other actions that you are required to take in response to a data breach under s 75 of the My Health Records Act.

Please sign and date this form on behalf of your organisation/agency.

s47F [redacted]

Signature: ..... Date: 12 DEC 17.

Name of signatory:

DOCUMENT 4

Australian Government

Office of the Australian Information Commissioner

My Health Record Data Breach Notification Form

Who should use this form?

This form is intended for use by the My Health Record System Operator, registered repository operators, healthcare provider organisations and registered portal operators who are required to report data breaches of the My Health Record System to the Office of the Australian Information Commissioner (OAIC) under s 75 of the *My Health Records Act 2012*. Further information on data breach reporting requirements and the actions that entities need to take in response to a breach are in the OAIC's guide to *Mandatory data breach notification in the My Health Record System*.

This form is not intended for entities voluntarily reporting data breaches to the OAIC. See *Data breach notification — A guide to handling personal information security breaches* for information on how to report data breaches that are not subject to mandatory reporting requirements.

Reporting My Health Record System data breaches

The System Operator, registered repository operators, healthcare provider organisations and registered portal operators are required to report data breaches to the OAIC as soon as practicable. It is not compulsory for entities to use this form to report a My Health Record System data breach to the OAIC. However, if you do not wish to use this form, you must notify the OAIC of the details requested below (where applicable).

The OAIC recognises that not all information requested on the form will be available when you first notify the OAIC of a data breach. Any information that you are unable to provide when making the initial report should be provided as it becomes available.

If you have any questions about this form or mandatory data breach reporting requirements, please email the OAIC Enquiries Line enquiries@oaic.gov.au or call 1300 363 992. Email contact is preferred.

Submitting this form

Please send the completed form by email to enquiries@oaic.gov.au, or by fax to (02) 9284 9666.

Information on actions the OAIC may take in relation to data breaches is available in the OAIC's guide to Mandatory data breach notification in the My Health Record System.

Organisation/agency details

Name of organisation/agency **Australian Digital Health Agency**

Is your organisation/agency: **My Health Record System Operator**

Contact officer details

Name: **Tony Kitzelmann**

Title/role within the organisation/agency: **General Manager and Chief Information Security Officer, Cyber Security Centre, Core Services Systems Operations Division**

Email: **anthony.kitzelmann@digitalhealth.gov.au**

Contact phone number: **(07) 3023 8421**

Please advise the OAIC as soon as possible of any change in contact details.

Details of the breach

Please provide the following details where available/applicable. Additional pages can be attached if required.

Description of the breach, outlining the suspected unauthorized collection, use or disclosure or threat to the security or integrity of the My Health Record System:

An individual with access to a Medicare Online Account can access their Medicare claims history and make a claim for the Medicare rebate online. As part of its compliance program, the Department of Human Services has identified fraudulent Medicare online claiming activity. If this activity has resulted in fraudulent claims being sent to the My Health Record System, these claims are removed from the My Health Record by the Department of Human Services and reported to the OAIC. The consumer is also notified of the removal of the incorrect or inaccurate claims by the My Health Record System Operator.

Following advice from the Department of Human Services that fraudulent Medicare claiming information has been sent to a My Health Record, the System Operator reviews all transactional information relating to that record to determine if any other online activity has occurred i.e access or viewing of information contained in the record.

In this case, evidence indicates that it is probable that the My Health Record was created using the myGov account used to conduct the online Medicare fraud. As it cannot be conclusively determined that both actions were performed by a third party and not by the consumer themselves, the System Operator is notifying the OAIC of a potential data breach.

When did the breach occur?
23 September 2013.

What type of personal information was involved in the breach?
Consumer demographics (name, address, DOB, age, IHI) and Medicare information.

How many consumers were or may have been affected? *(Do not include any personal information of consumers affected by the breach.)*
One.

What caused the breach? Please provide details of the preliminary assessment, and the outcomes of any further assessments as they are completed.
The breach was potentially caused by a person other than the legitimate owner of the My Health Record creating and accessing a My Health Record.

Was the breach inadvertent or intentional (for example, a deliberate act by an individual staff member)?
The breach occurred due to a deliberate act by a person other than the legitimate consumer.

When and how did your organisation/agency become aware of the breach?
The System Operator became aware of the breach on 16 November 2017 when transactional data became available.

Were any other entities involved in the breach?
The Department of Human Services.

Has your organisation/agency experienced a similar breach(es) in the past?
Yes

For registered repository operators and registered portal operators

Have you notified the System Operator of the breach?

☐ Yes

☐ No

Under s 75 of the My Health Records Act, registered repository operators and registered portal operators are required to notify both the System Operator and the OAIC. A civil penalty may apply if an entity does not notify both the OAIC and the System Operator as soon as practicable. On receiving a data breach notification, the OAIC will liaise with the System Operator to ensure that it has also received notification of the data breach.

Have you asked the System Operator to notify the affected consumer(s) (and the general public if a significant number of consumers were affected)?

☐ Yes

☐ No

For the System Operator

Have you notified the affected consumer(s) (and the general public if a significant number of consumers were affected)?

The Department of Human Services have contacted the consumer.

If yes, when and how was this notification provided? If no, when and how do you intend to notify affected consumers?

The Department of Human Services via mail.

The OAIC will contact you to discuss this notification and to seek further information if required. Please refer to the OAIC's guide to *Mandatory data breach notification in the My Health Record System* for further information on other actions that you are required to take in response to a data breach under s 75 of the My Health Records Act.

Please sign and date this form on behalf of your organisation/agency.

s47F [redacted]

Signature: ..... Date: 12 DEC 17

Name of signatory: