Australian Government
Australian Digital Health Agency

My Health Record
Managing Your B2B Software in Production

17 March 2020 v1.3

Approved for external use

Document ID: DH-3129:2020

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

OFFICIAL

Document information

Key information

Owner	Director System Management
Date of next review	10 September 2020
Contact for enquiries	Australian Digital Health Agency Help Centre Phone 1300 901 001 Email help@digitalhealth.gov.au

Table of contents

1 Introduction

1.1 Purpose

This document outlines the process for liaising with the My Health Record System Operator (SO) about production incidents and events requiring notification to the SO, such as changes and upgrades to software that connects to the My Health Record system.

1.2 Intended audience

This document is intended for Business-to-Business (B2B) software vendors.

2 Incident management

2.1 Incidents

An incident is any production issue related to software function, installation, certificate, connection or infrastructure issues which affects the functionality of a vendor's software. Such issues may cause data loss, incorrect information, display problems or a data breach associated with data transferred to and from the My Health Record system. Certain incidents need to be reported to the SO and these are outlined in *Section 2.4.2 Incident Types*.

2.2 Responsibilities

Vendors play a key role in the diagnosis and resolution of incidents. As per the obligations set out in the *My Health Records Act 2012* and *My Health Records Rule 2016*, you will be required to assist the SO by:

- reporting incidents including vendor software incidents or problems to the SO within two business days of their identification (refer to *Section 2.3 Contact Details*);
- undertaking or assisting in investigations to identify the root cause of an incident and if required, implementing a technical solution to fix an issue within your software;
- ensuring that an incident within your software is contained and where an immediate resolution is not possible, that an appropriate work-around is identified;
- providing and maintaining up to date contact details to the SO for relevant help desks, incident coordinators / managers, or other individuals (such as technical or security specialists) involved in the incident management process;
- communicating to customers, where appropriate, about the details of the problem and resolution in consultation with the SO;
- implementing, at your own cost, the remediation actions in the agreed timeframes for any incident;
- providing the SO with information required to inform post incident review reports;
- protecting the confidentiality of personal and health information held in the My Health Record system and treating the information in accordance with the Australian Privacy Principles contained in the Privacy Act 1988 and the My Health Record Act 2012; and
- notifying the SO when there are changes or upgrades to the software, refer to *Section 3 Software Changes and Upgrades* for more information.

The SO will:

- work cooperatively with vendors in resolving vendor software incidents and problems;
- where appropriate, transition unresolved vendor incidents to the SO's problem management process for root cause analysis and resolution; and

- communicate to vendors through Service Australia's Online Technical Support (OTS) team or the My Health Record website about system releases, relevant planned changes to the My Health Record system, changes to requirements and details of planned and unplanned outages.

2.3 Contact details

Vendors must report incidents, including vendor software incidents or problems within two business days of their identification to the SO via the following support contacts:

- **Business hours:** OTS Help Desk - **1300 550 115** or myhealthrecord.otshelpdesk@servicesaustralia.gov.au
- **After hours:** My Health Record Helpline - **1800 723 471** (Select option 2 and please make it clear that you have an incident relating to your My Health Record connection)

2.4 Incident management governance

2.4.1 Vendor incident management requirements

To access the My Health Record production environment, vendors shall be able to demonstrate that they have reasonable incident management processes in place to manage incidents as they arise.

2.4.2 Incident types

Table 1 describes the incident types that must be escalated to the SO for resolution and/or consultation. Initial triage will be performed by the SO Incident Manager before escalation to the appropriate functional area.

Table 1 - Incident Types

Type of incident	Description	Scenario examples
System Incident	An unplanned interruption to the My Health Record system's operations which results in a reduction or loss of system functionality.	• Major telecommunications failure.
Security Incident This type of event could also have compliance and privacy implications	A breach of the My Health Record system's security measures resulting in a threat to the integrity, availability, or confidentiality of the My Health Record system.	• Your software is compromised, and/or a vulnerability is exploited that affects multiple consumers. • A coordinated Denial of Service attack is identified. • Identifiable healthcare or personal data are exposed. • A vendor's software is infected with malware and starts leaking data out to a malicious user. • Secure communications between a vendor's software and the My Health Record system components is compromised. • A consumer identifies that an unrecognised person has accessed their record.

Type of incident	Description	Scenario examples
Clinical Safety Incident	An event or circumstance that resulted, or could have resulted, in unintended or unnecessary harm to a person.	• A healthcare provider advises that they believe a clinical document contains incorrect information for their patient. • Software is submitting data (e.g. clinical documents) to the My Health Record system which is associated with the wrong healthcare recipient.
Regulatory Incident/Breach This type of event may also have security and privacy implications	An identified breach of My Health Record policy, rules, regulations or legislation.	• A person overrides a healthcare recipient's access controls and views a clinical record without having grounds to do so.
Privacy Incident	My Health Record consumers have had their personal information collected, shared or used in an inappropriate way.	• A consumer identifies an unrecognised person or organisation in the access history of their My Health Record. • Medical information in a healthcare recipient's My Health Record is discussed widely by a vendor's staff without the healthcare recipient's consent. • Unauthorised access by another consumer.
Fraud Incident This type of event may also have security and privacy implications	Identified or potential deception intended to result in financial or personal gain.	• A vendor captures clinical data in transit and provides the de-identified data to a medical research company. • A vendor's system administrator with access to the system sells the IHIs of several high-profile individuals. • A vendor's system administrator with access to the system gathers individual's information from the My Health Record system to enable them to access services or payments.
Vendor Software Incident	Any issues with the functions or performance in the software.	• Trouble accessing or viewing information, incorrect information or missing information in the software. • Trouble acquisitioning or downloading the relevant information. • Trouble uploading clinical documents. • Trouble rendering clinical information. • Monitoring of the production environment and analysis of documents by the SO identifies non-conformance with mandatory requirements.

3 Software changes and upgrades

3.1 Software authentication and product type elements

All software products that are granted My Health Record production environment access for the first time must ensure the Product Type Reference values in the PCEHR header reflect the software version permitted to execute the transaction.

The PCEHR header is used for all interactions with the My Health Record system. The Product Type element identifies the system originating the request and contains the following fields that must represent the current system state that is transacting with the My Health Record system.

Element Name	Type	Cardinality	Remarks
productType		**1..1**	
vendor	String	1..1	client system's vendor name
productName	String	1..1	client system's product name
productVersion	String	1..1	client system's product version
platform	String	1..1	client system's platform
/productType			
clientSystemType	String	1..1	Values ("CCP","CPP", "CIS", "CSP", "CRP", "HI", "Medicare", "Other")

Software products that have previously been granted production access and have implemented a significant change (see *Section* *3.3 Significant interaction, transaction and administrative changes*) must re-declare and update the Product Type Reference Values.

Examples of populated Product Type Reference values in the PCEHR header have been provided below. The reference values accommodate a standard Clinical Information System software product, a product transacting through HIPS, and a product transacting through a Contracted Service Provider.

Standard software ProductType pattern:

```
<Product Type>
<Vendor>Example Software Pty Ltd</Vendor>
<ProductName>New Health Software</ProductName>
<ProductVersion>1.1</ProductVersion>
<Platform>Microsoft Windows NT 6.1.7601 Service pack 1</Platform>
</Product Type>
```

Software ProductType pattern for software transacting through HIPS:

```
<Product Type>
<Vendor>Jurisdiction or Organisation</Vendor>
<ProductName>HIPS</ProductName>
<ProductVersion>7.2</ProductVersion>
<Platform>Microsoft Windows NT 6.1.7601 Service pack 1</Platform>
</Product Type>
```

Note: The **<vendor>** string is constructed by populating the source system/solution's vendor name, product and version.

Software ProductType pattern for software transacting through a Contracted Service Provider:

```
<Product Type>
<Vendor>Source System Vendor or Organisation</Vendor>
<ProductName>CSP Product Name</ProductName>
<ProductVersion>1.0</ProductVersion>
<Platform>Microsoft Windows NT 6.1.7601 Service pack 1</Platform>
</Product Type>
```

Note: The **<vendor>** string is constructed by populating the source system/solution's vendor name, product and version.

For more detail on the PCEHR header, see the Logical and Technical Service Specifications available at the Australian Digital Health Agency website:

https://www.digitalhealth.gov.au/implementation-resources

3.2 Software registration in production

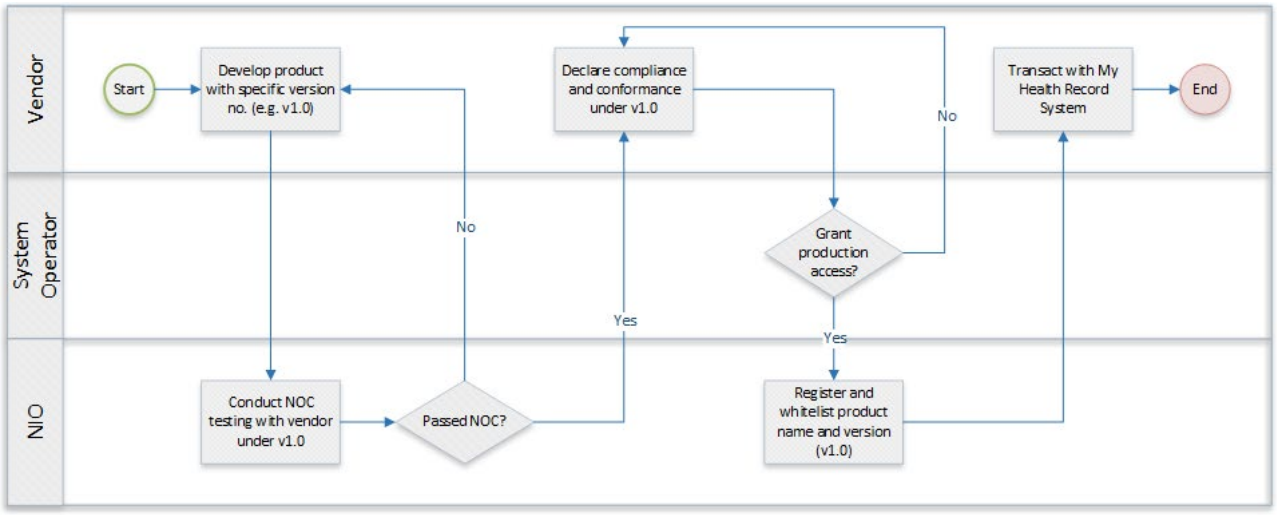
For a vendor software product to interact with the My Health Record system in production, the software product name and version must be registered by the National Infrastructure Operator (NIO). All transactions with the My Health Record system have the request header information validated against approved product details (name and version).

The production registration process involves the software vendor doing the following:

- completing Notice of Connection (NOC) testing with the NIO to demonstrate product functionality in conformance with the declared published standards
- submitting a completed Conformance Vendor Declaration Form to the SO.

For a description of the production registration process for a new vendor's software, refer to *Figure 1*.

Figure 1: Production registration process



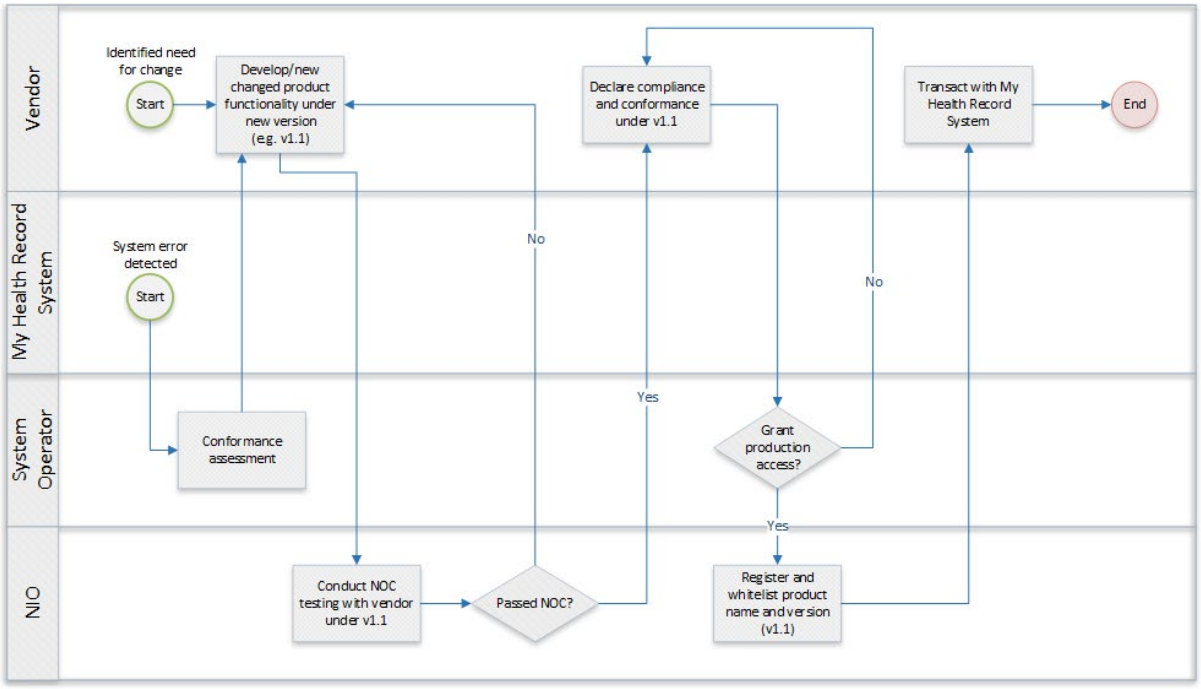
3.3 Significant interaction, transaction and administrative changes

A significant change is one which:

- makes functional or technical changes or upgrades that alters the way the software interacts or transacts with the My Health Record system; and/or
- impacts the software product's declared conformance to the requirements and specifications.

For a description of the process for a significant software change, refer to *Figure 2*.

Figure 2: Significant software change process



If you make a significant change to a software product connected to the My Health Record production environment, you:

1. Should advise the Digital Health Agency Help Centre at help@digitalhealth.gov.au with the subject line of *Vendor software change* and include the following information:
    - software details (vendor's name, contact details and software name)
    - new version number (if applicable)
    - proposed functionality change/s to the software
    - proposed release date.
2. Will need to regression test your software in the My Health Record Software Vendor Test (SVT) Environment.
3. In most cases, you must successfully re-complete NOC testing (*Section 3.4, Table 2* describes the various software changes requiring re-completion of NOC testing).
4. Must increment your software product version number. You are not permitted to introduce new functionality or material changes under previously approved product versions. For examples, see Section *3.4 Examples of significant software changes and upgrades*.
5. Will need to update the Product Type Reference values in the PCEHR header.
6. Will be required to submit a new *Conformance Vendor Declaration Form* notifying the SO of the change or upgrade.

    Note: To support declaring conformance to the My Health Record requirements, the *Conformance Vendor Declaration Form* contains a dialogue box to provide a detailed description of the software change or new functions.
7. Should email the Help Centre at help@digitalhealth.gov.au if clarification or support is required.

These requirements also apply to any fixes requiring a code change that address problems or incidents impacting the My Health Record system.

In the event a significant administrative change to your business, legal or support structure or software name occurs, email the Help Centre at help@digitalhealth.gov.au using the subject line: *Vendor administrative change,* including the confirmed details of the change/s.

3.4 Examples of significant software changes and upgrades

Table 2 outlines examples of significant software changes and the NOC testing and conformance declaration actions required.

Table 2 - Examples of significant software changes and upgrades

Description of change	**NOC testing**	**Clinical document NOC testing**	**Conformance declaration**	**Header update**[5]
Software calls an additional web service or makes changes to the existing web service.	Yes[1]	No	Yes	Yes
Software renders a new view or changes an existing view.	No[2]	No	Yes	Yes
Software produces an additional clinical document.	No	Yes	Yes	Yes
Change conformance profile and/or template id.	No	Yes	Yes	Yes
Software that transacts through the HIPS product and produces a Discharge Summary document conformance level 1A.	No	No[3]	Yes	No
Software that transacts through the HIPS product and produces any other clinical document type other than a Discharge Summary document conformance level 1A.	No	Yes	Yes	No
Software uses a different version of HIPS than initially declared.	No	No	Yes	Yes
Software change to conform to: • a clinical document conformance requirement • address a clinical document issue reported by the SO.	No	Yes	Yes	Yes
Introduction or change of a clinical terminology coding set to the clinical documents your software produces.	No	No[3]	Yes	No
Vendor de-scopes a function or service previously available. For example, no longer: • produces a clinical document • calls a web service • renders a view.	No [2]	No	Yes	Yes
Software change to address a web service problem or incident reported by the SO.	Yes	No	Yes	Yes
Software change to address a software interface problem or incident reported by the SO.	No[2]	No	Yes	Yes
Software change to conform to a mandatory software conformance requirement.	Yes[1]	No	Yes	Yes
Deprecation of a software version rendering the software or the specific version as obsolete and not able to access the My Health Record system.	No	No	Yes[4]	No

Description of change	NOC testing	Clinical document NOC testing	Conformance declaration	Header update[5]
Your organisation undergoes legal structure changes; is involved in a merger or acquisition; or nominated contact person(s), or their contact details change.	No	No	Yes	No
Release of a major or minor software version that *does not* alter the way the software interacts or transacts with the My Health Record system and does not impact adherence to your declared conformance with the requirements and specifications.	No	No	No	No[5]

[1] You must make use of our SVT environment to validate new functionality being introduced.

[2] You are strongly recommended to make use of our SVT environment to re-test changes made to your software.

[3] You are strongly recommended to send a sample document to the SO for validator testing.

[4] Advice to myhealthrecord.operations@digitalhealh.gov.au is required.

[5] Where the software SOAP header is updated, developers must perform a successful transaction in the SVT environment.

3.5 Insignificant interaction changes – localised bug fix version

If you make a change to your software that does ***not*** impact adherence to your declared conformance with the requirements and specifications and does ***not*** alter the way the software interacts or transacts with the My Health Record system, you should:

1. Regression test your software in the My Health Record SVT environment; and
2. Continue to transact with the previously provisioned access to the My Health Record system.

Note: Re-completion of NOC testing, update of the Product Type Reference values in the PCEHR header, and conformance declaration via a Conformance Vendor Declaration Form will not be required.

3.6 NOC testing and conformance requirements

If NOC testing and declaring conformance must be re-completed, the following will apply:

For **NOC testing**, you will need to:

- perform self-assessment testing of the changed or upgraded software functionality using either existing or new test cases and test data in the My Health Record Software Vendor Test (SVT) Environment and submit the 'self-assessment' test evidence for assessment
- attend a virtual session with the NIO to test the connectivity of the software with the My Health Record system, demonstrating that the software is functioning according to the declared conformance with the specifications.

For **clinical document upload to SVT**, you will need to:

- upload sample clinical document/s to the SVT environment
- inform the My Health Record operations team the IHI of the test patient/s, document ID/s and date and time of the document/s upload.

For **Conformance Vendor Declaration**, you will need to update and re-submit a *Conformance Vendor Declaration Form* to the SO, including:

- providing details of the software change or upgrade inclusive of all existing functionality
- declaring conformance to all mandatory My Health Record requirements relating to the functionality being delivered.

Once the above steps have been successfully completed, the SO will issue a *Production Environment Access Letter* to you, acknowledging that the updated software has been approved and granted access for specific transactions with the My Health Record system.

3.7 System Operator-initiated changes

New mandatory requirements or changes to the specifications and template packages may be updated or replaced from time to time and the SO may withdraw support for previous versions. Although the SO will endeavour to consult with affected vendors about any such changes, you will be required to keep your software up to date with the new or updated specifications and template packages.

To respond to SO-initiated changes, you are required to ensure the capability is present to deploy in an acceptable timeframe. Failure to do so may result in the software no longer having access to the My Health Record system.

System Operator-initiated changes, at a minimum, require a declaration of conformance, incrementing of the software version and may require NOC testing.

3.8 Support for software changes or upgrades

If a you are unsure whether you need to re-complete NOC testing and/or submit a new *Conformance Vendor Declaration Form* email the Help Centre at help@digitalhealth.gov.au using the subject line: *Vendor software change,* including the following information:

- software details (vendor's name, contact details and software name)
- new version number (if applicable)
- proposed functionality change/s to the software
- proposed release date.

3.9 More information

The My Health Record System Management team manages the day-to-day operational activities of the My Health Record system. For more information or assistance, please email: myhealthrecord.operations@digitalhealth.gov.au.

You may also find the My Health Record website useful: http://www.myhealthrecord.gov.au

Definitions

Term	Description
Business to Business (B2B)	The gateway that enables server to server connection and communication between the My Health Record system and connected systems, other than mobile/web applications.
Conformance declaration	The process where vendors declare conformance to national digital health specifications. This involves completing a *Conformance Vendor Declaration Form.*
HIPS	Health Identifier and PCEHR System. An integration product made available by the Australian Digital Health Agency to assist healthcare sites to integration with the Healthcare Identifier Service and My Health Record system.
Incident	An unplanned interruption or reduction in the functionality or availability of the My Health Record system and associated systems and services, which may include connecting apps.
Online Technical Support (OTS)	The first point of contact for software vendors. OTS helps software vendors diagnose and resolve technical issues during the testing and production stages.
National Infrastructure Operator (NIO)	The National Infrastructure Operator (NIO) is the business area responsible for providing and managing the My Health Record system on behalf of the System Operator.
Notice of Connection (NOC)	A notice issued by the My Health Record System Operator indicating that a system is ready to connect to the My Health Record system.
Notice of Connection (NOC) testing	NOC testing is the process of testing software using test cases and test data provided by the System Operator. Tests are executed in the My Health Record Software Vendor Test (SVT) environment and are verified by the NIO.
PCEHR	Personally Controlled Electronic Health Record. Former name for My Health Record.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem is created. A problem is handled by the problem management process which will further investigate and determine a root cause to support resolution of the problem.
Software Vendor Test environment (SVT)	The My Health Record system test environment managed by the National Infrastructure Operator (NIO) to facilitate functional and integration testing of developer apps in order to obtain a Notice of Connection (NOC).
System Operator	The System Operator is presently the Australian Digital Health Agency. It is responsible for establishing and operating the My Health Record system.
Vendor	Refers to any legal entity that develops and/or supplies software that enables individuals and/or healthcare providers to transact with the My Health Record system.