



Reference Platform

Vendor End 2 End Portal

Solution Design

Version 1.4

23 August 2012

Confidential - Draft

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au**Disclaimer**

NEHTA 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. NEHTA 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. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright © 2012, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Table of contents

Table of contents	iii
Document information	iv
Change history	iv
Approved	iv
1 Introduction	1
1.1 Background.....	1
1.2 Purpose.....	1
1.3 Definitions, acronyms, abbreviations.....	1
1.3.1 Terminology	1
2 Portal Access	2
2.1 Website	2
2.2 Certificates	2
2.3 Portal Authentication and Authorization.....	2
2.4 Portal Home Page	3
3 File Store	4
3.1 All Files	4
3.2 My Files.....	5
3.3 Upload New File.....	6
4 Message Delivery Status.....	7
4.1 Deliver option in the Uploaded Files section	7
4.2 Message Delivery Status	8
5 File Viewer.....	9
6 Sealed Message Delivery (SMD) Endpoint.....	11
6.1 Healthcare Identifiers Service Lookup	11
6.2 Endpoint Location Service Lookup	12
6.3 Secure Message Delivery	12
6.4 PCEHR Document Upload Service	13

Document information

Change history

Doc Version	Date	Author	Comments
1.0	03 Oct 2011	Kai Loke	Draft
1.3	20 Aug 2012	Andrew Ireland	Revision due to addition of PCEHR Document Upload service. Screen shots updated to reflect refinements.

Approved

Date	Approved	Signature

This page is intentionally left blank.

1 Introduction

1.1 Background

The Reference Platform is an environment used to test, implement, demonstrate and verify aspects of the NEHTA work program.

1.2 Purpose

This document describes the design for a Vendor End 2 End Portal on the External Reference Platform (XRP). The purpose of the portal is to enable collaboration and end to end testing between parties implementing the NEHTA specifications stack.

The functionality of the portal will include (and not be limited to):

- The ability for jurisdictions and vendors to upload and share generated CDA documents, CDA zip documents (packaged using the XDM profile) and HL7 v2 MDM messages for the purpose of verification and testing.
- A CDA package viewer which will allow vendors to upload and view contents of CDA zip documents packaged using the XDM profile.
- Delivery of CDA Packages through SMD and HL7 v2 MDM messages through the use of HL7 v2 clients (Argus, HealthLink, Global Health) or SMD-compliant clients.
- A CDA document/package upload service that permits vendors to programmatically upload a document via a web service. The service returns a SOAP response object specifying whether the upload succeeded, and if it not, the reasons and/or warnings for the failure.

1.3 Definitions, acronyms, abbreviations

CDA	Clinical Document Architecture
EJBCA	Enterprise Java Bean Certificate Authority
MDM	Medical Document Management
NASH	National Authentication Service for Health
NEHTA	National E-Health Transition Authority
SMD	Secure Message Delivery

1.3.1 Terminology

The keywords **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** in this document are to be interpreted as described in IETF's RFC 2119 [RFC2119].

2 Portal Access

2.1 Website

The Vendor End 2 End portal is located at this URL:

<https://portal2.xrp.nehta.org.au/VendorEnd2End/>

Browser support:

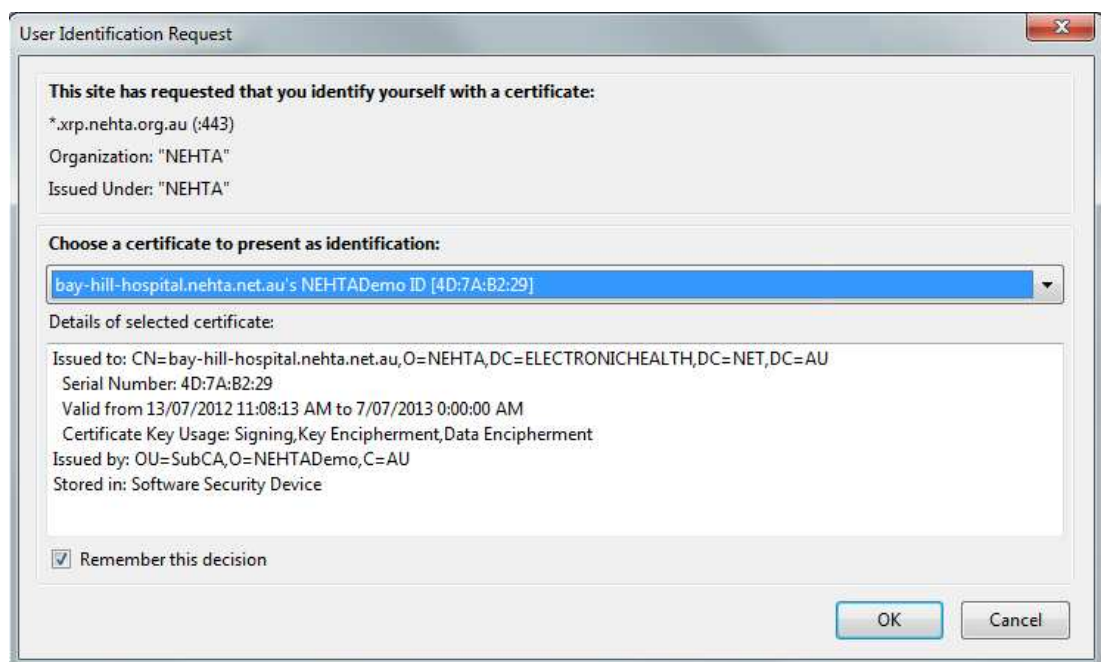
- 1) Mozilla Firefox (all versions)
- 2) Internet Explorer 8.0. For version 9.0, *Compatibility Mode* has to be turned on for XML to be rendered correctly.

2.2 Certificates

Vendors will be accessing the End 2 End Portal using NASH issued test certificates. Users will be identified by the HPI-O number available on the certificate.

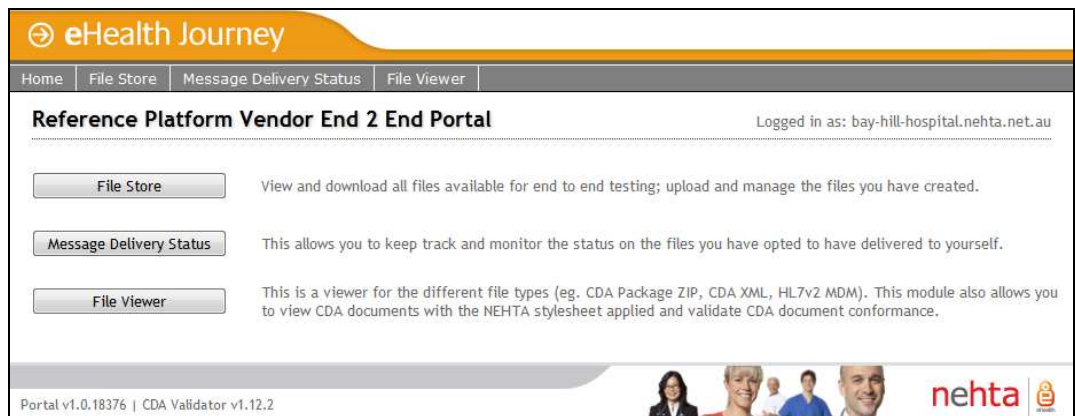
2.3 Portal Authentication and Authorization

Upon logging onto the portal for the first time, users will be prompted to present a certificate for identification. Once authenticated, the user will then be directed onto the portal home page.



2.4 Portal Home Page

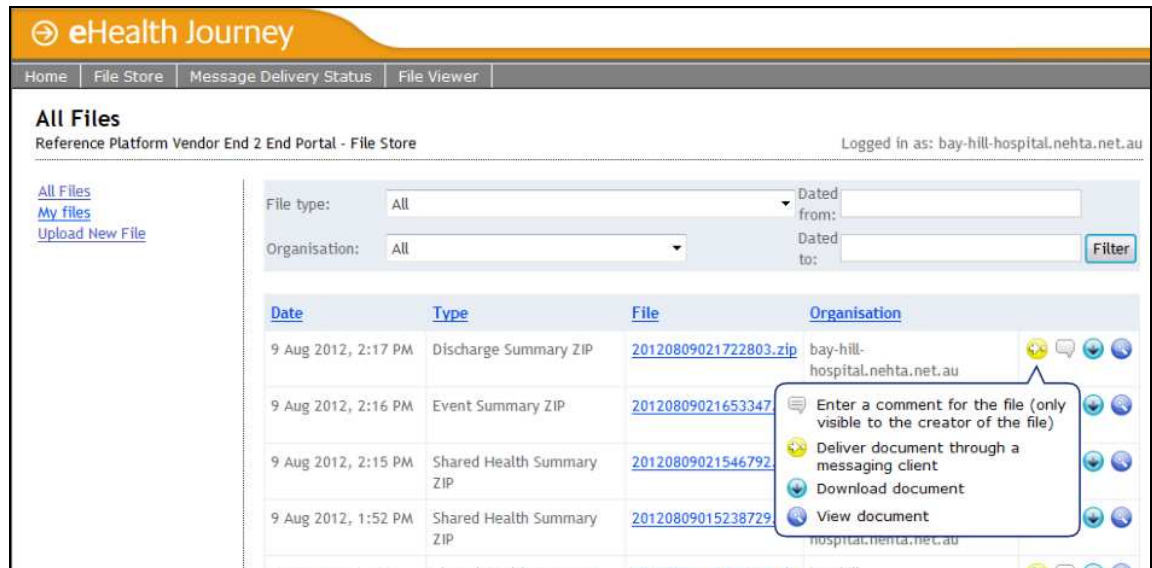
The portal home page contains a menu of the modules / functionality available on the portal.



3 File Store

This section serves as a document repository for the purpose of document sharing between vendors implementing NEHTA specifications. Users will be able perform different functions (validate, view, deliver, etc) on documents created by other users to test for conformance and interoperability.

3.1 All Files



This page displays a list of all the files that have been collectively uploaded by all organisations. Filters can be applied on organisation, file type and date on the list. Users have the option of downloading the files, or to view them online. Clicking on the file name will toggle a display of the description below it (as shown in the second entry in the above screenshot).

Certain actions will be file type specific. For instance, against a CDA XML document, there will be an option to validate the file.

Users will also be able to submit comments against the files. This is to facilitate the provision of feedback. A messaging vendor having received and parsed an eReferral CDA ZIP file successfully, may make a comment approving the file. A single file attachment can be added with each comment, to facilitate feedback such as a screenshot of what the CDA document looks like with their product.

For instance, a GP vendor wishing to complete end-to-end testing for a Discharge summary will do the following:

- 1) Select to deliver (to themselves) the discharge summary document through a messaging client;
- 2) Render the document upon receipt;
- 3) Take a screenshot of the locally rendered document and upload it against the discharge summary document with a comment to indicate that it was successful. This enables jurisdictions to know that their documents have been created correctly and can be rendered by their intended recipients.

As another example, jurisdictions wishing to complete end-to-end testing for eReferrals will perform the same actions - select the eReferral document to deliver (to themselves); render the document locally, and finally to screenshot the output and upload it along with comments against the eReferral document as feedback for the file.

3.2 My Files

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

My Files
Reference Platform Vendor End 2 End Portal - File Store

Logged in as: bay-hill-hospital.nehta.net.au

[All Files](#)
[My files](#)
[Upload New File](#)

File type: All Dated from: Dated to: [Filter](#)

Date	Type	File	Organisation
10 Aug 2012, 2:27 PM	Shared Health Summary ZIP	20120810022702707.zip	bay-hill-hospital.nehta.net.au
10 Aug 2012, 2:18 PM	EReferral CDA	EReferral_3A_Min.xml	bay-hill-hospital.nehta.net.au
10 Aug 2012, 2:17 PM	Discharge Summary ZIP	20120810021731216.zip	bay-hill-hospital.nehta.net.au
10 Aug 2012, 2:16 PM	Event Summary ZIP	20120810021653763.zip	bay-hill-hospital.nehta.net.au
10 Aug 2012, 2:15 PM	Shared Health Summary ZIP	20120810021552170.zip	bay-hill-hospital.nehta.net.au
10 Aug 2012, 2:12 PM	Discharge Summary ZIP	20120810021349500.zip	bay-hill-hospital.nehta.net.au

Enter a comment for the file (only visible to the creator of the file)
Deliver document through messaging client
Download document
View document
Delete

This page displays all the files created by the organisation that is logged in. Filters can be applied to the list similar to the **All Files** page.

The *Comment* icon displays the comments received for the file.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

My Files
Reference Platform Vendor End 2 End Portal - File Store

Logged in as: bay-hill-hospital.nehta.net.au

[All Files](#)
[My files](#)
[Upload New File](#)

20120810021731216.zip [Close](#)

type: Discharge Summary ZIP date: 10 Aug 2012, 02:17 PM organisation: bay-hill-hospital.nehta.net.au

Andrew from bay-hill-hospital.nehta.net.au - 3:21 PM, 14 Aug 2012
I received this file successfully almost immediately, however when rendering it in my software I found some strange characters appearing in the output. Please see screenshot attached to see what I'm talking about...

Attachment included (C:\Data\FileStore_Test.jpg)

Add New Comment

Test date:

User name:

Comment:

Attachment: [Browse...](#) Accepted file types: jpg, gif, pdf - Maximum file size: 500kb

[Add Comment](#)

Portal v1.0.18214 | CDA Validator v1.12.2

nehta

3.3 Upload New File

The screenshot shows the 'Upload New File' page within the 'eHealth Journey' portal. The page has a navigation bar with links: Home, File Store, Message Delivery Status, and File Viewer. The main heading is 'Upload New File' with a sub-header 'Reference Platform Vendor End 2 End Portal - File Store'. The user is logged in as 'bay-hill-hospital.nehta.net.au'. On the left, there are links for 'All Files', 'My files', and 'Upload New File'. The main form area contains fields for 'UploadFile:' (with a file path 'C:\Data\Checkout\PCEHR' and a 'Browse...' button), 'Name:' (with the text 'EReferral_3A_Min.xml'), and 'Description:' (with the text 'EReferral minimum XML set.'). A 'Create' button is at the bottom of the form. The footer shows 'Portal v1.0.18214 | CDA Validator v1.12.2' and the 'nehta' logo.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

Upload New File
Reference Platform Vendor End 2 End Portal - File Store

Logged in as: bay-hill-hospital.nehta.net.au

[All Files](#)
[My files](#)
[Upload New File](#)

UploadFile: C:\Data\Checkout\PCEHR

Name: EReferral_3A_Min.xml

Description: EReferral minimum XML set.

Portal v1.0.18214 | CDA Validator v1.12.2

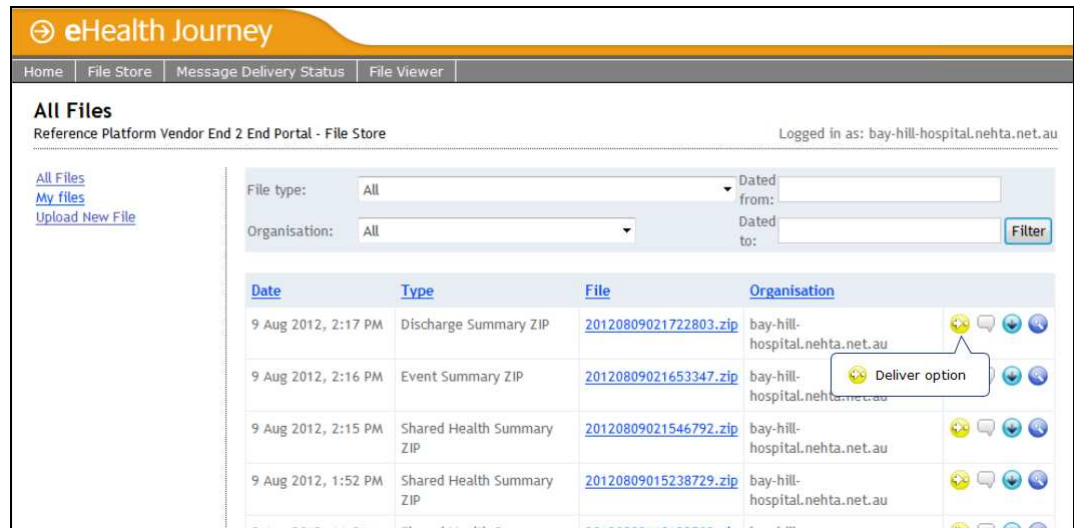
nehta

This page allows users to upload new files. A file type can be selected from a list to describe the content of the file (ePrescription, Shared Health Summary, etc). A description of the file can also be entered which will be displayed in the **All Files** page.

4 Message Delivery Status

In the **All Files** section, users can select files to be delivered to themselves via HL7v2 clients like Argus, HealthLink, Global Health, and also through Sealed Message Delivery (SMD).

4.1 Deliver option in the Uploaded Files section

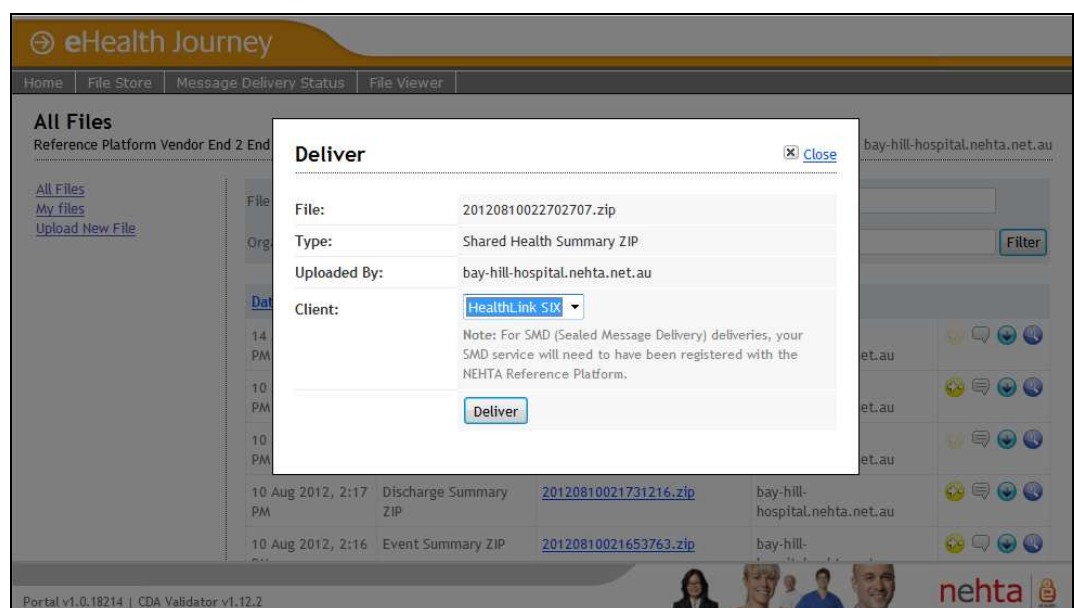


When the deliver option is selected, a popup will appear allowing the user to select the delivery client. The uploaded file will then be delivered via the selected client to the organisation (via the organisation's HPIO number).

The list of messaging clients planned to be supported at this time are:

- HealthLink
- Global Health
- Argus
- SMD (Sealed Message Delivery)

As mentioned, the document can also be delivered via SMD. Your SMD service endpoint will need to have been registered with the Reference Platform.



4.2 Message Delivery Status

Once a file has been selected to be delivered, it will appear in a list under the **Message Delivery Status** page. The list can be filtered by organisations, file types and date of delivery. Delivery statuses on individual files are also indicated in the list.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

Message Delivery Status
Reference Platform Vendor End 2 End Portal

Logged in as: bay-hill-hospital.nehta.net.au

File type: All Dated from: Dated to: Filter

Organisation: All

Delivery Date	Client	Status	Type	File	Organisation
14 Aug 2012, 3:32 PM	HealthLink SIX	Pending	Shared Health Summary ZIP	20120810022702707.zip	bay-hill-hospital.nehta.net.au
14 Aug 2012, 3:30 PM	Argus V6	Delivered	Discharge Summary ZIP	20120810021731216.zip	bay-hill-hospital.nehta.net.au
14 Aug 2012, 3:29 PM	HealthLink SIX	Delivered	Shared Health Summary ZIP	20120810022702707.zip	bay-hill-hospital.nehta.net.au
14 Aug 2012, 3:29 PM	HealthLink SIX	Delivered	Shared Health Summary ZIP	20120810022702707.zip	bay-hill-hospital.nehta.net.au
14 Jun 2012, 2:35 PM	HealthLink SIX	Delivered	Shared Health Summary ZIP	20120614120527879.zip	bay-hill-hospital.nehta.net.au
14 Jun 2012, 2:35 PM	Argus V6	Delivered	Shared Health Summary ZIP	20120614120527879.zip	bay-hill-hospital.nehta.net.au
14 Jun 2012, 2:34 PM	HealthLink SIX	Delivered	Shared Health Summary ZIP	20120614120527879.zip	bay-hill-hospital.nehta.net.au
14 Jun 2012, 2:34 PM	SMD	TRD Success	Shared Health Summary ZIP	20120614120527879.zip	bay-hill-hospital.nehta.net.au

Portal v1.0.18214 | CDA Validator v1.12.2

Clicking on the comment icon (as shown above) will display a popup with all the comments that the current logged-in organisation has submitted for that file. The user will be able to submit a new comment with the option of including a file attachment.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

Message Delivery Status
Reference Platform Vendor End 2 End Portal

Logged in as: bay-hill-hospital.nehta.net.au

File type: All Dated from: Dated to: Filter

Organisation: All

20120810021731216.zip [Close](#)

type: Discharge Summary ZIP date: 10 Aug 2012, 02:17 PM organisation: bay-hill-hospital.nehta.net.au

Andrew from bay-hill-hospital.nehta.net.au - 3:21 PM, 14 Aug 2012
I received this file successfully almost immediately, however when rendering it in my software I found some strange characters appearing in the output. Please see screenshot attached to see what I'm talking about...

[Attachment included \(C:\Data\FileStore_Test.jpg\)](#)

Add New Comment

Test date:

User name:

Comment:

Attachment: [Browse...](#) Accepted file types: jpg, gif, pdf - Maximum file size: 500kb

[Add Comment](#)

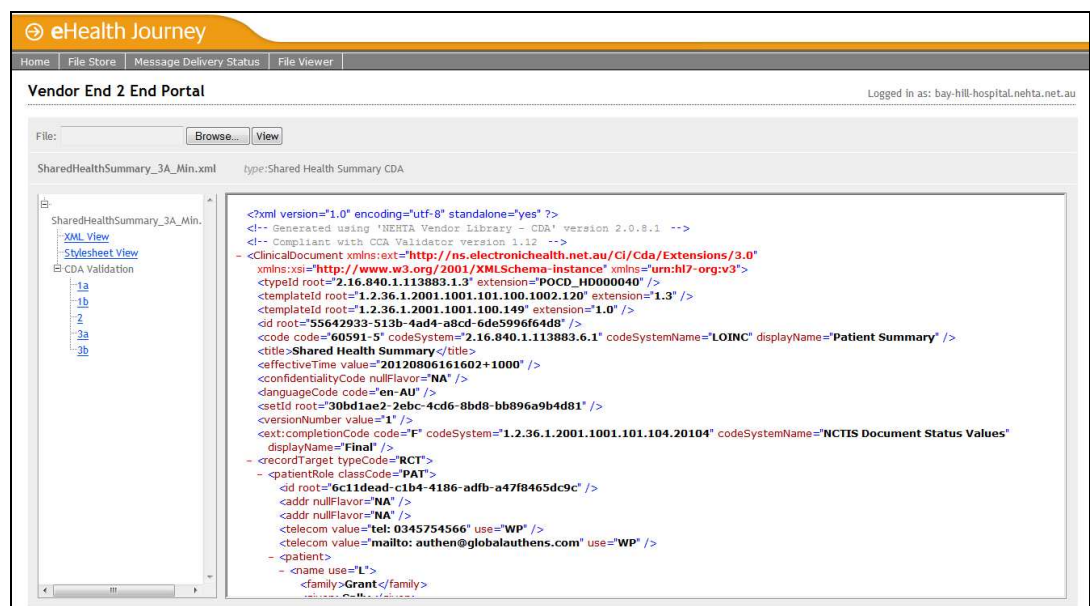
Portal v1.0.18214 | CDA Validator v1.12.2

5 File Viewer

This section serves as a tool for viewing CDA XML files, CDA package ZIP files and HL7 v2 MDM files. If it is a CDA package ZIP file, a message will be displayed to indicate if the signature on the CDA package zip file can be verified.

The user will be able to view a list of the content of the file, as well as to view individual files. For CDA documents, users will be provided with options to :

- View the raw XML;
- View the document with the NEHTA style sheet applied;
- Validate the CDA document according to conformance levels 1a, 1b, 2, 3a and 3b.



The above example shows the viewer with a CDA document XML file. The user has the option to view the XML (xml view, pictured above), view with the NEHTA style sheet applied (Stylesheet view) and to apply CDA validation over the document.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

Vendor End 2 End Portal Logged in as: bay-hill-hospital.nehta.net.au

File: Browse... View

SharedHealthSummary_3A_Min.xml type:Shared Health Summary CDA

SharedHealthSummary_3A_Min.

- XML View
- Stylesheet View**
- CDA Validation
 - 1a
 - 1b
 - 2
 - 3a
 - 3b

Shared Health Summary

PATIENT: Miss Sally Wally GRANT SEX: Female DOB: 6 Aug 1955 AGE: 57 years

☒ Administrative Details ☒ Provider Identifiers **IHI**

START OF DOCUMENT

PATIENT DETAILS

Name	Miss Sally Wally GRANT a.k.a. Mr Wally GRANT	Document Type	Shared Health Summary
Sex	Female	Creation Date/Time	6 Aug 2012 10:00:00
Date of Birth	6 Aug 1955 (57 years)	Date/Time Attested	Not Attested
IHI	8003 6023 4868 7602	Document ID	556
Local Identifiers	542181 (Croydon GP Centre) 1234567891 (Medicare Card Number)	Document Set ID	306
Address	No Fixed Address	Document Version	1
Contact	Phone: 0345754566 (Workplace) Email: authen@globalauthens.com (Workplace)	Completion Code	Final
		Author	Smith, John
		Author Contact	Phone: 0345754566 Email: authen@globalauthens.com
		Author Address	No Fixed Address
		Author Organisation	Global Health Solutions

Adverse Reactions

Exclusion Statement

Exclusion Statement

None known

This example shows the viewer with a CDA file. Here, the **Stylesheet view** is chosen, which renders the CDA document with the NEHTA style sheet applied.

Clicking on a CDA validation level will display a report indicating the presence and location of any errors.

eHealth Journey

Home | File Store | Message Delivery Status | File Viewer

Vendor End 2 End Portal Logged in as: bay-hill-hospital.nehta.net.au

File: Browse... View

EReferral_3A_Min.xml type:EReferral CDA

EReferral_3A_Min.xml

- XML View
- Stylesheet View
- CDA Validation
 - 1a
 - 1b
 - 2
 - 3a
 - 3b

CDA Validator Report

VALIDATION STATUS	Complete
SERVICE NAME	e-Referral - 1b
SERVICE PROVIDER	NEHTA
STANDARD TYPE	CDA R2
STANDARD VERSION	N/A
DATE OF TEST	20120814
TIME OF TEST	162916.0728 +1000
REPORT POSITIVE INDICATOR	True
RESULT OF TEST	Passed
ERROR COUNT	0
WARNING COUNT	0

Test Object

```
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:ext="http://ns.electronichealth.net.au/C1/Cda/Extensions/3.0" xmlns:
<typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3" />
<templateId extension="2.2" root="1.2.36.1.2001.1001.101.100.1002.2" />
<templateId extension="1.0" root="1.2.36.1.2001.1001.100.149" />
<id root="79a2fbfb-dbb6-47cb-aba6-d091756c381e" />
<code code="57133-1" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC" displayName="Referral Note" />
<title>e-Referral</title>
<effectiveTime value="20120806161600+1000" />
<confidentialityCode nullFlavor="NA" />
```


6 Sealed Message Delivery (SMD) Endpoint

The portal will host a Sealed Message Delivery service, which can be invoked to submit a document up to the **File Store**. The service endpoint can be discovered and invoked through a series of look ups:

- 1) Healthcare Identifiers Service lookup for the organisation "Bay Hill Hospital" (HPIO: 8003620000020052) – Bay Hill Hospital is a NEHTA test organisation. This will return the Endpoint Location Service endpoint.
- 2) Endpoint Location Service lookup for the organisation, service category and service interface. This will return the SMD service endpoint, along with the encryption certificate.
- 3) With the encryption certificate, the payload can then be encrypted and delivered to the Vendor End 2 End portal SMD endpoint.

6.1 Healthcare Identifiers Service Lookup

Healthcare Identifiers Service Endpoint:

<https://portal.xrp.nehta.org.au/MCAR3/ProviderSearchForProviderOrganisation/Service.svc>

HPIO:

<http://ns.electronichealth.net.au/id/hi/hpio/1.0/8003620000020052>

Sample code:

Request

```
searchHIPProviderDirectoryForOrganisation rpo =  
    new searchHIPProviderDirectoryForOrganisation();  
  
rpo.hpioNumber =  
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/8003620000020052";
```

Response

```
searchHIPProviderDirectoryForOrganisationResponse response =  
    client.searchHIPProviderDirectoryForOrganisation(  
        ref prod,  
        ref sc,  
        ts,  
        user,  
        hpio,  
        rpo);  
  
string elsURL = response.searchHIPProviderDirectoryForOrganisationResult  
    .organisationProviderDirectoryEntries[0]  
    .endpointLocatorService[0]  
    .serviceAddress;
```

6.2 Endpoint Location Service Lookup

Endpoint Location Service Endpoint:

<https://portal.xrp.nehta.org.au/ELS2010/LookupTls/Service.svc>

Service Category:

<http://ns.electronichealth.net.au/pcehr/sc/PutDocument/2011>

Service Interface:

<http://ns.electronichealth.net.au/smd/intf/SealedMessageDelivery/TLS/2010>

Target:

<http://ns.electronichealth.net.au/id/hi/hpio/1.0/8003620000020052>

Sample code:

Request

```
listInteractions request = new listInteractions();
request.interactionRequest = new nehta.ELSV2010.InteractionRequestType();
request.interactionRequest.serviceCategory =
    "http://ns.electronichealth.net.au/pcehr/sc/PutDocument/2011";
request.interactionRequest.serviceInterface =
    "http://ns.electronichealth.net.au/smd/intf/SealedMessageDelivery/TLS/2010";
request.interactionRequest.target =
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/8003620000020052";
```

Response

```
InteractionType[] response = client.listInteractions(request);
string smdURL = response[0].serviceEndpoint;
string certQual = response[0].certRef[0].useQualifier;
string certType = response[0].certRef[0].qualifiedCertRef.type;
string certValue = response[0].certRef[0].qualifiedCertRef.value;
```

6.3 Secure Message Delivery

Sealed Message Delivery Endpoint:

<https://portal2.xrp.nehta.org.au/VendorEnd2End/SMD/Service.svc>

Sample code:

Request

```
deliver request = new deliver();
request.message = new nehta.smd2010.SMD.SealedMessageType();

//Payload
EncryptedPayloadType ep = new EncryptedPayloadType();
request.message.encryptedPayload =
    (EncryptedPayloadType) DeserialiseElementToClass(payload.DocumentElement, ep);

//Metadata
request.message.metadata = new MessageMetadataType();
request.message.metadata.creationTime = DateTime.Now.ToUniversalTime();
request.message.metadata.invocationId = new UniqueId().ToString();
request.message.metadata.receiverOrganisation =
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/8003620000020052";
request.message.metadata.senderOrganisation =
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/800362xxxxxxxxxx";
request.message.metadata.serviceCategory =
    "http://ns.electronichealth.net.au/pcehr/sc/PutDocument/2011";
request.message.metadata.serviceInterface =
    "http://ns.electronichealth.net.au/smd/intf/SealedMessageDelivery/TLS/2010";
```

```
//To receive a TRD populate routeRecord
request.message.metadata.routeRecord = new RouteRecordEntryType[1];
request.message.metadata.routeRecord[0] = new RouteRecordEntryType();
request.message.metadata.routeRecord[0].interaction = new InteractionType();
request.message.metadata.routeRecord[0].interaction.serviceCategory =
    "http://ns.electronichealth.net.au/pcehr/sc/PutDocument/2011";
request.message.metadata.routeRecord[0].interaction.serviceEndpoint =
    "URL of your TRD endpoint";
request.message.metadata.routeRecord[0].interaction.serviceInterface =
    "http://ns.electronichealth.net.au/smd/intf/TransportResponseDelivery/TLS/2010";
request.message.metadata.routeRecord[0].interaction.serviceProvider =
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/800362xxxxxxxxxx";
request.message.metadata.routeRecord[0].interaction.target =
    "http://ns.electronichealth.net.au/id/hi/hpio/1.0/800362xxxxxxxxxx";
request.message.metadata.routeRecord[0].sendIntermediateResponses = false;
```

Response

```
deliverResponse response = client.deliver(request);
response.status = DeliverStatusType.ok
```

6.4 PCEHR Document Upload Service

The PCEHR document upload service is provided to vendors as a means of programmatically validating CDA documents and packages.

The following example is supplied as a guide to show the creation and sending of document upload requests utilising the vendor library.

Details of connection errors, validation errors and validation warnings will be returned within the members of the registry response object.

PCEHR Document Upload Service Endpoint:

<https://portal2.xrp.nehta.org.au/VendorEnd2End/PCEHR/DocumentRepositoryService.svc>

For more detailed information regarding the registry response object and the document exchange process, please refer to the PCEHR Document Exchange Service Technical Service Specification document found at the Nehta Software Developers Resource Centre (<https://vendors.nehta.gov.au>)

Sample code:

Request

```
// Obtain the certificate for use with TLS and signing
X509Certificate2 cert = X509CertificateUtil.GetCertificate(
    "Serial Number",
    X509FindType.FindBySerialNumber,
    StoreName.My,
    StoreLocation.CurrentUser,
    true
);

// Create PCEHR header
CommonPcehrHeader header = PcehrHeaderHelper.CreateHeader();

// Create the client
UploadDocumentClient uploadDocumentClient = new UploadDocumentClient(
    new Uri("https://UploadDocumentEndpoint"), cert, cert);

// Add server certificate validation callback
ServicePointManager.ServerCertificateValidationCallback +=
    ValidateServiceCertificate;

byte[] packageBytes = File.ReadAllBytes("CdaPackage.zip"); // Create a package
```

```
// Create a request from an existing package
ProvideAndRegisterDocumentSetRequestType request =
uploadDocumentClient.CreateRequestForNewDocument (
    packageBytes,
    FormatCodes.SharedHealthSummaryConformance3A,
    HealthcareFacilityTypeCodes.Transport,
    PracticeSettingTypes.SpecialistMedicalPractitionerServiceNEC
);
```

Response

```
try
{
    // Invoke the service
    RegistryResponseType registryResponse =
uploadDocumentClient.UploadDocument (header, request);

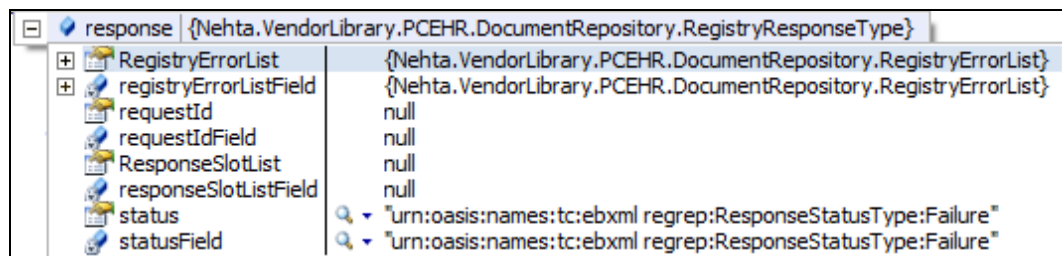
    // Get the soap request and response
    string soapRequest = uploadDocumentClient.SoopMessages.SoopRequest;
    string soapResponse = uploadDocumentClient.SoopMessages.SoopResponse;
}
catch (FaultException fex)
{
    // Handle any errors
}
```

PCEHR Document Upload Service Errors/Warnings

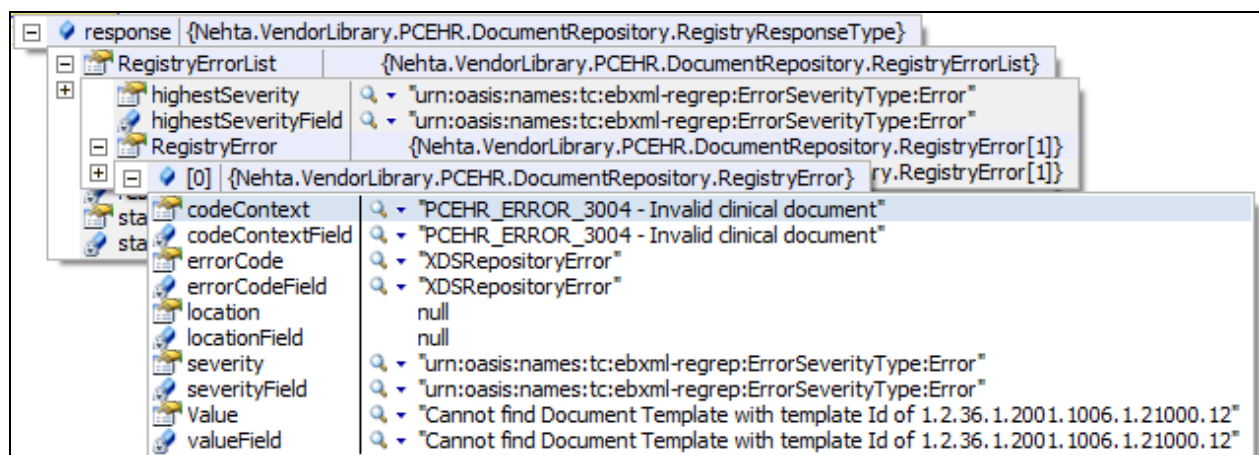
The registry response object will indicate the success or failure of the upload.

If the document upload is successful, the registry response object will return a status "success" status. Also, the document will appear on the File Store page for further viewing.

If the document upload fails, detailed information as to why it failed will be returned in the registry response object.



This example shows a registry response object that has a failed status.



As you can see, individual errors and/or warnings are returned in the `RegistryErrorList` member of the registry response.