# NHIN Direct Demo



## NHIN Direct Demo

## Scenarios

### Scenario 1

---

More detail on "specialist sends summary care information back to referring provider"

Summary care information resides in PODS service (or equivalent) that supports PODS MIM and interfaces (at the moment get() and getByII()

The physician credential is the only credential that can access the PODS record

In the scenario, the specialist HISP receives the outcomes record from PODS either as XML or CDA, if the former, it converts to CDA.

Specialist uses GAARDS to authenticate and authorize transfer and to manage PKI to encrypt payload.

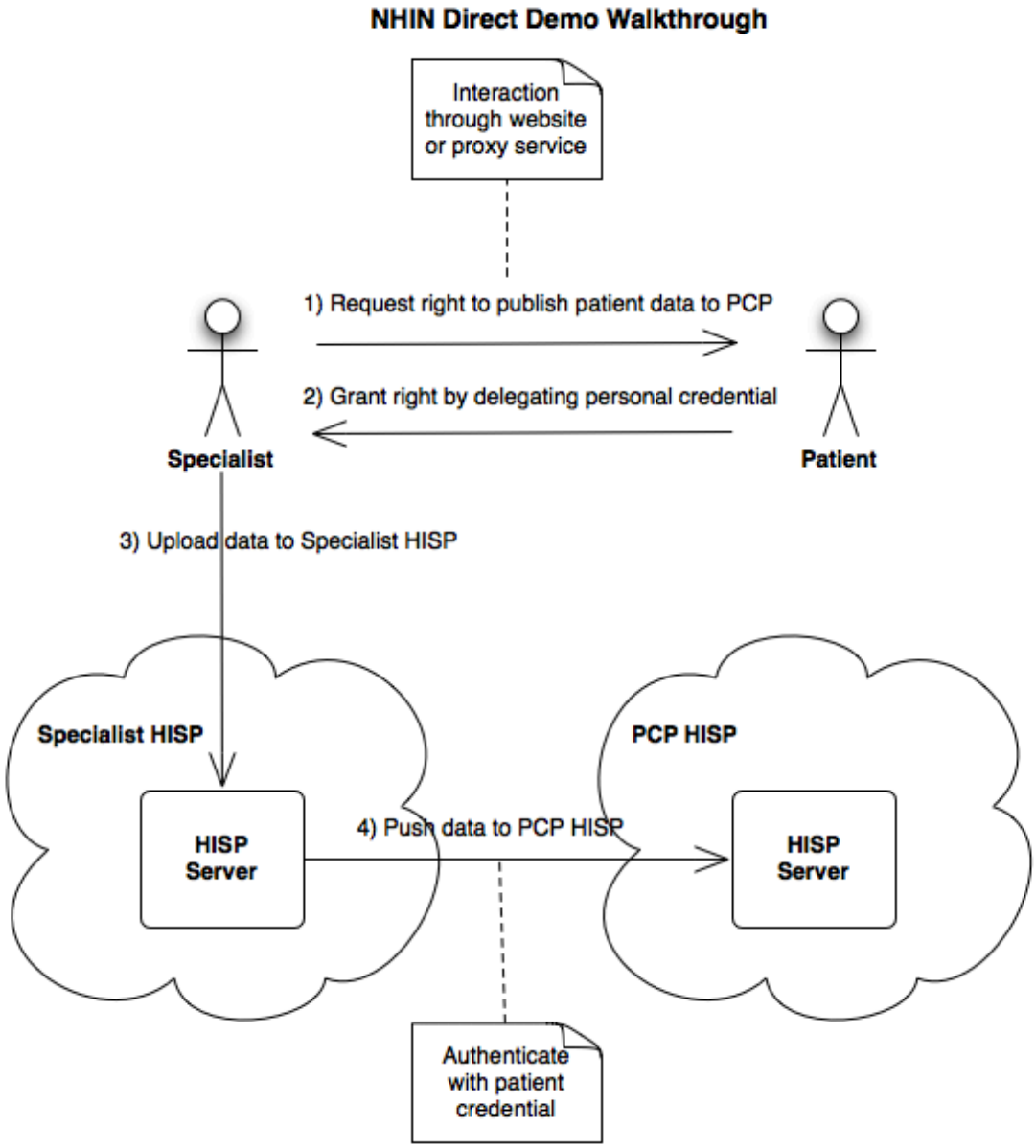
HISP sends CDA packaged document and style sheet to receiving HISP

Receiving HISP uses GAARDS to manage PKI artifacts to decrypt payload.

Sophisticated receiving HISP (Kaiser Permanente or DOD) directly decodes and integrates CDA based data into their EHR

Less sophisticated groups (Dr. Bob) opens in browser using style sheet to visualize

This use case demonstrates interactions with both high and low capability recipients, and demonstrates how use of GAARDS and CRUX enables reasonable security without the need for individuals to manage PKI artifiacts.




1. a. Specialist has PCP's public key
   b. Specialist HISP and PCP HISP trust each other's CA
2. Scenario summary:
   a. Specialist needs to publish updated patient record to referring PCP.
   b. Specialist and PCP do not directly communicate, but rather use HISP servers.
3. Workflow with security
   a. Specialist requests permission from user to transfer the updated record to the PCP
   b. User consents and signs a token with his public key.
   c. Specialist signs the updated record using his credential, and encrypts it using the PCPs public key.
   d. Uploads the payload, secured patient record and token to the Specialist HISP.
   e. Specialist HISP validates this message: does the user allow this transfer, is the message secured correctly (per abstract model, The HISP ensures the authenticity, integrity and confidentiality of the message in a way that traces the provenance of the message to the Source)
   f. Specialist HISP sets up a SSL connection with PCP HISP using its credential, mutually authenticated.
   g. Payload is sent over a SSL channel, with data privacy.
   h. PCP HISP stores the secured payload for PCP access
   i. PCP validates message:
      i. uses his private key to decrypt the payload, and Specialist's public key to verify validity of payload.
      ii. validates token to ensure Specialist has right to push the data.
4. Notes for demo:
   a. Assume provisioning of keys as out-of-band operation, ideally would be some form of registry
   b. Token as SAML Authorization Assertions, that are stored on a server that releases the token to any one who queries.
   c. Both HISPs could have certificates from same CA, but s/w will easily support different CA per HISP.
   d. Specialist HISP validating the message could be simple checks to see if message is signed by trusted specialist and encrypted.

e. UI should have a way for Specialist or PCP to just say validate or sign/encrypt, and provide key passphrase without any PKI exposed to user.

# Actors

1. Patient - But he doesn't do much, he just has a credential in this demo and that credentials allows one to read and publish data to the PCP's health service
2. PCP - The primary care physician
3. Specialist - Enough said

# Services

1. Specialist Health Portal - Web UI + RESTful service for editing and sending patient data
2. PCP Health Portal - Web UI + RESTful service for storing and receiving patient data and viewing messages from specialist
3. SAML Service - RESTful service for obtaining SAML assertions .

In actuality, the Specialist and PCP health servers will be the same code deployed on 2 instances.

# Workflow

1. Specialist goes to Specialist Demo Login Page, enters (username &?) password and clicks "Login". The result is that the Specialist Health Portal now has a copy of an active credential for the Specialist cached in the portal. (Transacation 1.1)
2. Specialist will get directed to Patient Data Page.
3. Specialist will edit & click "Save" to save mock patient data on the Specialist Health Portal
4. Specialist will then click "Send" on the same page to send patient data to PCP Health Portal on the Specialist Health Portal.(Transaction 1.2)
5. Specialist will be re-directed to the Patient Credential Delegation Page that represents a workflow for getting approval from patient to share data with PCP. In our demo, it will simply a page that shows a simple form for creating a SAML assertion using the simulated Patient's credentials. (This is our additional capability)
6. Once an assertion has been delegated a message containing the patient's latest data will be created and sent to the PCP Health Portal. The user will be re-directed back to the Edit Patient Data Page as part of this process.(This is our additional capability)
7. PCP goes to PCP Demo Login Page, enters (username &?) password and clicks "Login". The result is that the PCP Health Portal now has a copy of an active credential for the Specialist cached in the portal. (Transactions 3.1
8. PCP will load a screen to view messages generated by the specialist and will see a list of messages with the status of "Read" or "Unread".
9. The PCP will click on the newest unread message and be able to see the patient's data and who sent the data. The message will now be marked "Read". (Transactions 2.1, 2.2, 2.3)

Note: The specialist should be able to send more messages like this without having to be re-directed for as long as credential is active or until the demo person goes back to the "Start Demo" page and clicks "Start Demo"

## UI the specialist will use

1. Start Demo Page - Landing page for demo, clicking on start demo will destroy any active delegated credential in the demo
2. Patient Data Form - UI for viewing / editing patient data, sending data to PCP Health Portal and will probably show a status field whether a credential has been delegated
3. Patient Credential Delegation Page - UI for delegating a credential to the Specialist. Will require us to enter mock patient's password to create proxy

## UI the PCP will use

1. View Health Service Messages List
2. View Health Service Message

Note: There is a lot more we could do for UI, but this is a demo only. Even the re-direct is overly fancy but I like having it in this demo because it communicates in an elegant way that the specialist needs to be granted permission to share the patient's data.

## References


1. http://nhindirect.org/NHIN+Direct+Abstract+Model
2. http://confluence.globus.org/display/CRUX/NHIN+Direct+Security+Notes
3. NHIN Direct Implementation WG F2F Presentation Slides from NHIN Direct F2F