Technical Agreement

Exchanging FHIR Data using a generic Notified Pull mechanism

Versie: 0.99

Disclaimer: For Trial Implementation

Table of contents

1 Introduction

This Technical Agreement (TA) describes and specifies technical responsibilities to which parties agree when connecting to exchange transactions to facilitate the Notified Pull.

The possibility to exchange a patient's medical record is for example required in case of a patient referral or transfer. When different healthcare organizations are involved in a patient’s treatment plan, attention should be paid to the required legal permission and the possible ‘burden’ for the Receiving System when a medical record is transferred.

The Notified Pull provides a solution for the “Legal Push”, where data is transferred from one organization to another. The Notified Pull transaction expects that in case of a patient referral the Receiving Organization is carefully selected by the Sending Organization. This action confirms the treatment relationship between the patient and the future healthcare provider and can be seen as an “presumed permission”. The patient is aware of the referral and therefore understands that their medical records will be transferred.

Receiving a medical record with a traditional Push transaction was found to be of concern for the Receiving System, for several reasons. The Notified Pull will inform (notify) a Receiving Organization of medical records that are ready to be collected (including the patient’s required permission). The Receiving Organization only receives on its own terms, by controlling how and when to execute the Pull operations that were suggested by the Sending Organization.

1.1 Goal, scope, and principles

The goal of this document is to introduce a neutral, objective design for the exchange of FHIR resources using the Notified Pull exchange pattern. To achieve full technical interoperability using this exchange pattern, integration partners must have made agreements on the following topics:

- Protocol and syntax of Notification and Pull interactions
- Authorization of FHIR resource endpoints
- Registration, discovery and exchange of identifiers, addresses and public keys of systems
- Registration, discovery and exchange of identifiers and human readable attributes of healthcare organizations
- Identification and authentication of natural persons

This document provides normative specifications for the first two topics (in chapters 2, 3, and 4). Additionally, this document provides non-normative guidelines for the implementation of topics 3, 4 (in chapter 5) and 5 (in section 3.4). To achieve full technical interoperability, system vendors must make additional agreements on these last three topics based on the guidelines provided in this document.

The following principles are followed in this document:

- The design must use international standards.
- The design should be as generic and sustainable as possible (with a life cycle of at least 3-5 years).
- The design should be reusable for multiple use-cases.
- The design should strive to reuse methods and components from existing health exchange infrastructures (e.g., MedMij, NUTS, Twiin, LSP AORTA)
- The design must comply or explain. If anything deviates based on earlier principles, this can only be done if the reason is explained. This could be a deviation of use of standards, principles or if parts of the design are not reusable.
- The design should not contain more specifications than what is strictly necessary within the goal and scope of this document.

This document does not define which systems within the source are responsible for the creation, storage, or maintenance of any specific dataset. Neither will this document address the use-cases that drive the need to exchange that dataset as there are many programs in the Netherlands that already do so. Instead, this document will focus on the roles and responsibilities a system or systems may have to get that dataset from a Sending Organization to a Receiving Organization using FHIR.

1.2 Context

The initial reason for drawing up this generic technical agreement is the need for a FHIR specification for the exchange of the BgZ (Basisgegevensset Zorg) between healthcare organizations in the context of a referral. The actual agreements for the exchange of the BgZ are provided in the BgZ attachment. The exchange of the BgZ is not the first use-case that requires a FHIR specification for the exchange of a set of FHIR resources between healthcare organizations in the context of a transfer of care. The eOverdracht information standard and corresponding TA cover a similar use-case and already provide a specification for the exchange of FHIR resources using a Notified Pull pattern. As such, the relevant specifications in the eOverdracht information standard and TA have served as a basis for this document. At some points this document deviates from the eOverdracht information standard and TA (most specifically in the exchange of the Notification). Where it deviates, it does not aim to replace the existing version of the eOverdracht standards and corresponding implementations. It rather aims to provide a direction for the next iteration of the eOverdracht information standard and TA.

1.3 Definition of terms

Term	Definition
BgZ	“Basisgegevensset Zorg”, the Dutch interpretation of the International Patient Summary.
Dataset	A set of patient information which needs to be exchanged based on the Notified Pull.
eOverdracht	A Nictiz information standard to facilitate a nursing transfer.
Organization	Healthcare organization.
Receiver Pull	A more formal designation of the Pull.
Receiving Organization	The receiving organization/party.
Receiving System	The system for the receiving (electronic health record) organization.
Sending Organization	The sending organization/party.
Sending System	The system for the sending (electronic health record) organization.
System	Node or API-service provider for healthcare organizations.

1.4 Benefits of the Notified Pull

In comparison to a regular Push pattern, the Notified Pull pattern has the following benefits:

- The Receiving Organization only receives on its own terms, by controlling how and when to execute the Pull operations that were suggested by the Sending Organization. This allows for data minimisation by (if applicable and possible) only asking what you want to receive, when you want to receive it.
- The Receiving Organization can potentially have access to more up-to-date data, because the data can be pulled at the very moment the information is actually needed.
- The Notified Pull mechanism allows for a deeper layer of security. When a user of the Receiving Organization wants to retrieve the medical data, the user needs to identify itself. In comparison, using a regular Push, the data will directly be sent to the Receiving System, without the possibility to identify which users of the Receiving Organization are accessing that data.
- Implementations of the Notified Pull pattern can be reused when implementing a regular Pull pattern.

In comparison to a regular Receiver Pull pattern, the Notified Pull pattern has the following benefits:

- In relation to a regular Receiver Pull, the Notified Pull mechanism allows for better timing and security. With a regular Pull the Receiving System will have to continuously Pull to discover new information. Using a Notification to initiate a Pull reduces network communications and better timing by communicating when the message is ready to be received.
- A regular Receiver Pull requires an explicit registration of patient consent. Explicit consent registration is not required for a regular Push, nor is it required for a Notified Pull. It is not to be expected that all patients who require a transfer of information between healthcare providers will explicitly register a generic consent for Pull requests.

1.5 Relation to other documents

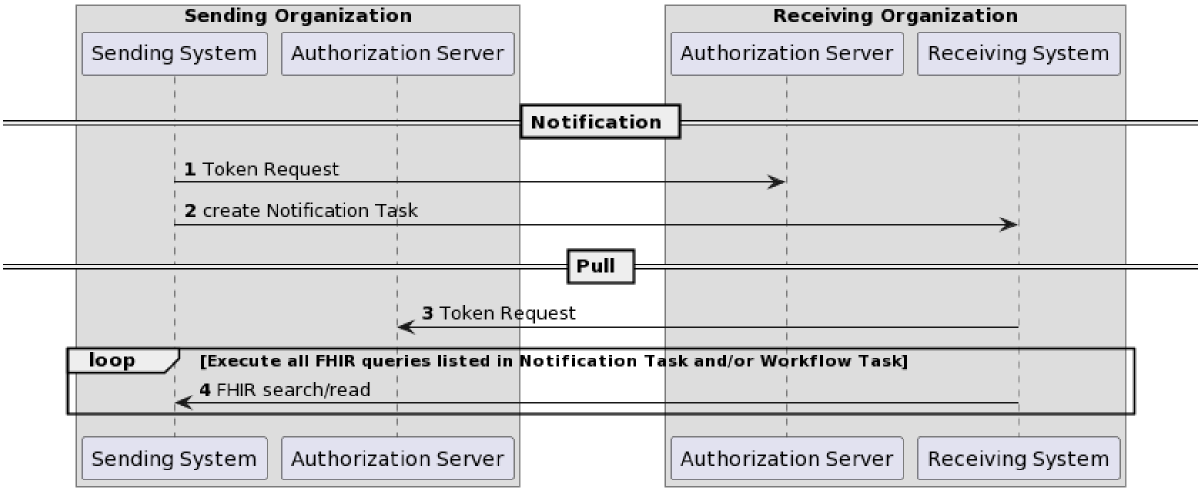
This document is written with the following documents as reference:

- Nictiz - Informatiestandaard BgZ MSZ
- TSV - Technical Agreement Exchanging BgZ

1.6 Format of Technical Agreement

The format of this Technical Agreement follows the main interactions as presented below in the simplified sequence diagram of the Notified Pull sequence.

Notified Pull using OAuth and FHIR



Interaction numbers 1 and 3 are described in the chapter Access control. Interaction number 2 is described in the chapter Notified Pull interactions. A part of interaction number 4 is also described in the chapter Notified Pull interactions, for specifics of the context of the Notified Pull see Nictiz information standards.

The chapter Full interaction sequence provides a complete sequence diagram that covers both the resource interactions and the authorization interactions of the complete Notified Pull interaction sequence.

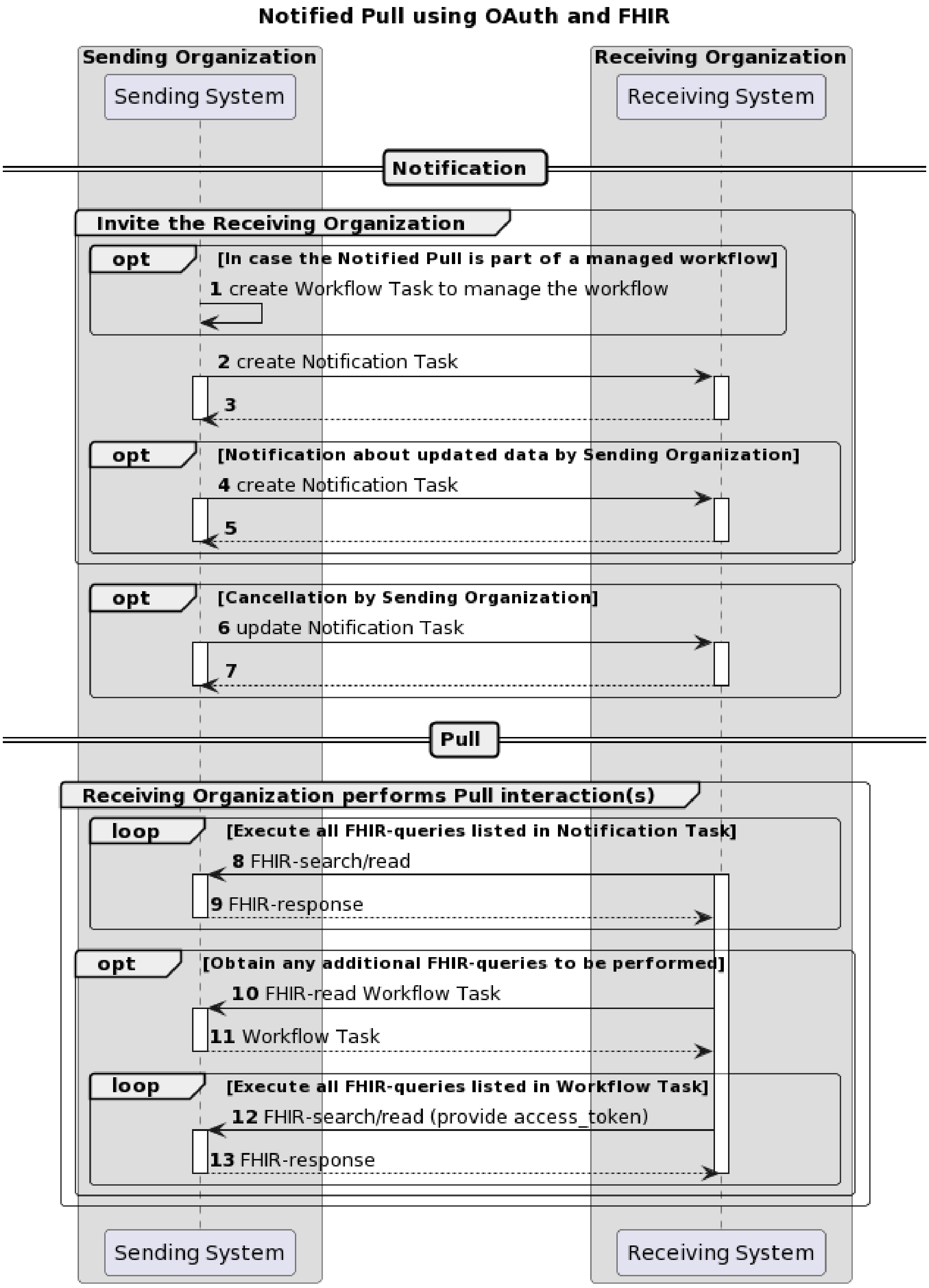
The chapter Identification and addressing provides non-normative information about solutions for identification and addressing.

2 Notified Pull interactions

This chapter describes all relevant interactions for the Notified Pull interaction sequence on data level.

2.1 Notified pull interaction sequence

All relevant interactions for the Notified Pull interaction sequence on data level are displayed in the sequence diagram below.


Notified Pull using OAuth and FHIR
Sending Organization
Sending System
Receiving Organization
Receiving System
Notification
Invite the Receiving Organization
opt
[In case the Notified Pull is part of a managed workflow]
1 create Workflow Task to manage the workflow
2 create Notification Task
3
opt
[Notification about updated data by Sending Organization]
4 create Notification Task
5
opt
[Cancellation by Sending Organization]
6 update Notification Task
7
Pull
Receiving Organization performs Pull interaction(s)
loop
[Execute all FHIR-queries listed in Notification Task]
8 FHIR-search/read
9 FHIR-response
opt
[Obtain any additional FHIR-queries to be performed]
10 FHIR-read Workflow Task
11 Workflow Task
loop
[Execute all FHIR-queries listed in Workflow Task]
12 FHIR-search/read (provide access_token)
13 FHIR-response
Sending System
Receiving System

Description of the interactions in this sequence diagram:

Steps	Description
1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR "Workflow Task" at the Sending System, then the flow starts with a creation of this Task on the Sending System. See Notification Task vs Workflow Task for additional details.
2-3	The Sending System invites the Receiving System to perform one or more Pull interactions (FHIR requests) by sending a FHIR Task resource ("Notification Task") to the Receiving System using a FHIR create interaction. See Notification message for a detailed description. The Receiving System processes the invitation and sends a technical response to complete the create interaction. See Notification response for a detailed description.
4-5	When the data set for which a Notification message has been sent is updated in the Sending System, the Sending System must inform the Receiving System about this update by sending a new Notification Message. See Notification message for a detailed description. The Receiving System processes the invitation and sends a technical response to complete the create interaction. See Notification response for a detailed description.
6-7	The "Cancellation by Sending Organization" option provides a means for the Sending System to cancel or revoke an erroneously created Notification. The Sending System communicates the cancellation to the Receiving System by sending an updated Notification Task to the Receiving System using a FHIR conditional update interaction. See Notification Cancellation message for a detailed description. The Receiving System processes the interaction and sends a technical response to complete the conditional update interaction. See Notification response for a detailed description.
8-9	The Receiving System extracts the intended FHIR requests from the Notification Task listed in Task.input:read-available-resource and Task.input:query-available-resources. Subsequently, the Receiving system initiates these FHIR requests and processes the responses.
10-11	In case that the Notification Task contains an indication that there is a Workflow Task at the Sending System that contains additional FHIR requests (i.e. when Task.input:get-worflow-task.valueBoolean is `true`), the Receiving System requests the Workflow Task at the Sending System.
12-13	The Receiving System extracts the intended FHIR requests from the Workflow Task. Subsequently, the Receiving system initiates these FHIR requests and processes the responses.

125

2.2 Notification message

The Notification message is sent by the Sending System when it needs to notify the Receiving System about one or more FHIR resources that have been made available to the Receiving System.

The Notification that is sent to the Receiving System must be able to convey at least the following details:

- Identification of Sending System, Sending Organization and practitioner
- Identification of Receiving Organization
- Identification of the patient who is the subject of information exchange
- References to individual FHIR resources that have been made available at the Sending System
- FHIR search queries that can be used to retrieve FHIR resources that have been made available at the Sending System
- Authorization base (see Authorization base)

The payload of this message consists of a FHIR STU3 Task[1] resource that contains at least the details mentioned above. This message is sent to communicate both a new and an updated data set to the Receiving System. The message results in a Task instance that will be referred to as the Notification Task.

The Sending System must initiate the Notification message using a FHIR create interaction, i.e. sending an HTTP POST request to the Task endpoint of the Receiving System.

The media type of the HTTP body must be either `application/fhir+json` or `application/fhir+xml`.

When generating the Notification message, the Sending System must set the Task attributes as specified in the table below. For complete information on constructing a FHIR Task Resource, see https://hl7.org/fhir/stu3/task.html.

[1] For the time being, the STU3 version of the FHIR standard will be used because this TA will first be applied in the context of the BgZ (Basisgegevensset Zorg). Within that context, data is exchanged based on FHIR STU3. As soon as data has to be exchanged using the Notified Pull pattern for newer FHIR versions, it becomes opportune to provide or adopt a specification of the Notification for the corresponding FHIR version.

Attribute	Card.	Description
basedOn	0..*	Optional reference to a request-Type resource that produced this event. If a workflow has been initiated and a Workflow Task is present, this must be referenced.
groupIdentifier	1..1	Unique identifier of the data set that is made available. An update to an existing data set at the Sending System triggers a new Notification Task, and thus a new Notification Task instance. Multiple Notifications Tasks on the same data set must share one unique identifier so that the Receiving System can identify them as relating to the same data set at the Sending System.
identifier	**1..1**	Business identifier of the task. This is a required field for traceability and cancellation of individual Notifications.
status	1..1	The state communicated by this event[2]. Fixed value: ● requested
intent	1..1	Indicates the "level" of actionability associated with the Task[3]. Preferred value: ● proposal
code.coding	**1**..1	A code briefly describing what the task involves: ● system = "http://fhir.nl/fhir/NamingSystem/TaskCode" ● code = "pull-notification"
restriction.period	0..1	The period during which the data will be available for retrieval.
requester.agent.identifier	1..1	Identifier of the system that initiated the Notification.
requester.onBehalfOf. identifier	**1**..1	Identifier of the Organization at which the data has been made available.
owner.identifier	**1**..1	Identifier of the Receiving Organization.
input:authorization-base	0..**1**	The authorization base to be used when retrieving the data. Constraints: ● type.coding ○ system = "http://fhir.nl/fhir/NamingSystem/TaskParamater" ○ code = "authorization-base". ● valueString
input:get-workflow-task	0..1	An indicator to show whether or not all available resources are part of this Notification. Constraints: ● type.coding ○ system = "http://fhir.nl/fhir/NamingSystem/TaskParameter" ○ code = “get-workflow-task” ● valueBoolean Where valueBoolean: ● true, the basedOn Workflow Task must be retrieved to get all available resources; ● false, all available resources are available in the next (two) input slices.

[2] See also: https://hl7.org/fhir/stu3/valueset-request-status.html
[3] See also: https://hl7.org/fhir/stu3/valueset-request-intent.html

Attribute	Card.	Description
input: read-available-resource	0..*	The FHIR-read interactions that can be performed to retrieve the data that was made available. Constraints: ● type.coding (one of:) ○ *Generic typing:* ■ system = "http://fhir.nl/fhir/NamingSystem/TaskParameter" ■ code = "read-resource" ○ *SNOMED CT typing:* ■ system = “http://snomed.info/sct” ■ code = a SNOMED CT code ○ *LOINC typing:* ■ system = “http://loinc.org” ■ code = a LOINC code ● valueReference format: ○ [resourcetype]/[id] Where: ● resourcetype denotes a FHIR resourcetype; ● id represents a logical id of a FHIR resource instance.
input: query-available-resources	0..*	The FHIR-search interactions that can be performed to retrieve the data that was made available. Constraints: ● type.coding (one of:) ○ *Generic typing:* ■ system = "http://fhir.nl/fhir/NamingSystem/TaskParameter" ■ code = "search-resource" ○ *SNOMED CT typing:* ■ system = “http://snomed.info/sct” ■ code = a SNOMED CT code ○ LOINC typing: ■ system = or “http://loinc.org” ■ code = a LOINC code ● valueString format: ○ [resourcetype]{?[parameters]} Where: ● resourcetype denotes a FHIR resourcetype; ● parameters can be added to refine a FHIR-search.

The Sending System MAY choose not to list the available FHIR resources in Task.input. In that case, the Sending System MUST provide a reference to a Workflow Task resource in Task.basedOn. This Workflow Task MUST list the available FHIR resources in Task.input, in the same format that is specified for the Notification Task. Additionally, in this case the Notification Task MUST have an entry in Task.input with the following values:

- Task.input.type.coding.system: "http://fhir.nl/fhir/NamingSystem/TaskParameter"
- Task.input.type.coding.value: “get-workflow-task”
- Task.input.valueBoolean: true

The Receiving System must accept both media types `application/fhir+json` and `application/fhir+xml`.

On receiving the submission, the Receiving System must validate the resource and respond with one of the HTTP codes defined in the Notification response.

The Notification should trigger an event in the Receiving System to process the expected Pull.

Persistence of the Notification Task as a FHIR resource is not necessary.

When the data set for which a Notification message has been sent is updated in the Sending System, the Sending System must inform the Receiving System about this update by sending a new Notification Message. In this case, Task.input:read-available-resource and Task.input:query-available-resources should only list the updated FHIR resources. This way, the update can be communicated as a delta to the original data set. This relieves the Receiving System of determining which resources have changed in a larger set of resources. Note that the value of Task.identifier for the new Notification Task must differ from the value of Task.identifier Notification Task for the original data set, while the value of Task.groupIdentifier must be the same for all Notification Tasks on the same dat set. This way, consecutive Notification Tasks on the same data set can be related to each other by the value of Task.groupIdentifier.

Note that the choice for the use of a Task resource as the Notification payload deviates from the eOverdracht specifications for the Notification (the eOverdracht specifications require the payload to be empty). The reasons for using a Task resource as Notification payload over an empty payload are that:

- It enables the Sending System to communicate the patient identifier and all available resources without providing a Workflow Task resource
- It enables the Sending System to communicate specific search queries that can be used to retrieve FHIR resources that have been made available to the Receiving System.
- It enables the Sending System to communicate updates in a dataset as a delta. This relieves the Receiving System of determining which resources have changed in a larger set of resources.
- It enables the Sending System to provide an authorization base in the Notification. As such, the Notification can be used as the distribution mechanism for the authorization base (see Authorization base).

2.3 Notification response

This message must be provided when a success or error condition needs to be communicated in response to an inbound Notification message. Success is only indicated once the Notification is received and completely processed.

To enable the Sending System to know the outcome of technical / syntactic processing of the Notification Task, the Receiving System must return either an empty body or an OperationOutcome resource. This body must be accompanied with the correct HTTP status code, e.g.:

- 200 OK – Notification received and not persisted.
- 201 Created – Notification received and persisted. In this case http-headers `Location` and `Etag` should be filled.
- 400 Bad Request – Notification could not be parsed or failed basic FHIR validation rules.
- 404 Not Found – Resource type not supported, or wrong endpoint.
- 412 Precondition Failed – The processing of the Notification Task could not be finished, since the criteria were not selective enough.
- 422 Unprocessable Entity – The Notification Task resource violated applicable server business rules. This should be accompanied by an OperationOutcome resource providing additional detail.

Whether or not the resources in input can be retrieved shall not be a factor in the HTTP status.

The Sending System processes the response according to application defined rules.

2.4 Notification Task vs Workflow Task

The FHIR Task resource used in the Notification payload is not meant to track the status of a workflow or healthcare process that initiated the data exchange. When the data that is exchanged using the Notified Pull pattern serves for instance a patient referral or transfer, the status of that process should be tracked using a separate FHIR Task resource that is maintained and hosted by the initiator of that process, i.e. the Sending System. To keep a clear distinction between these two Task resources, the Task resource used as Notification payload is referred to as the “Notification Task”, while the Task resource that is used to track a healthcare process or workflow is referred to as a “Workflow Task”. The Notification Task is sent from the Sending System to the Receiving System using a Push interaction (HTTP POST or PUT), while the Workflow Task is hosted at the Sending System, and can be requested by the Receiving System using a Pull interaction.

The use of a Notification Task as Notification payload does not require the presence of a Workflow Task, but when a Notification Task is sent in the context of a workflow that is maintained by the initiator of that workflow using a Workflow Task, the Notification Task MUST contain a reference to that Workflow Task.

2.5 Notification Cancellation message

The Notification Cancellation message is sent when the Sending System needs to send a cancellation of a previous Notification to the Receiving System. Just as the Notification message, the payload of this message consists of a FHIR STU3 Task resource.

The Sending System can cancel a previous Notification using a conditional update interaction on the Task that represents that previous Notification. This is done by sending an HTTP PUT request to the Task endpoint of the Receiving system, where the value of Task.identifier of that previous Notification is included in the query parameters of the PUT request.

The media type of the HTTP body must be either `application/fhir+json` or `application/fhir+xml`.

When generating the Notification Cancellation message, the Sending System must set the Task attributes as specified in the table below. For complete information on constructing a FHIR Task Resource, see https://hl7.org/fhir/stu3/task.html.

Attribute	Card.	Description
identifier	**1..1**	Business identifier of the Notification Task; the value of this identifier must be equal to the value of the identifier of the Notification Task that is to be cancelled.
status	1..1	The state communicated by this event. Fixed value: ● cancelled
intent	1..1	Indicates the "level" of actionability associated with the Task[4]. Preferred value: ● proposal

The Receiving System must accept both media types `application/fhir+json` and `application/fhir+xml`.

On receipt of the submission, the Receiving System must validate the resource and respond to the cancellation message according to the requirements specified in Notification response.

The Notification should trigger an event in the Receiving System to cancel any intended Pull interaction.

Persistence of the Notification Task as a FHIR resource is not necessary.

[4] See also: https://hl7.org/fhir/stu3/valueset-request-intent.html

2.6 Availability of BSN

For correct handling the BSN should be available as soon as possible, when this is legally required. The Sending System has two possibilities:

- The BSN is sent in the authorization assertion used in the access token request before sending the Notification Task.
- The BSN is made available through the Workflow Task resource which is referenced in the basedOn attribute of the Notification Task resource. The Workflow Task resource must have a for reference with the identifier filled with the BSN.

The Receiving System must support both. Since both variants are possible for the Sending System to use, both must be supported by the Receiving System, to be able to process from any Sending System.

3 Access control

Both the Sending System and Receiving System expose endpoints that must be protected from unauthorized and malicious interactions. More specifically, access control measures must be applied to the following endpoints:

- Receiving System: Notification endpoint (FHIR Task endpoint)
- Sending System: Resource endpoint

3.1 Network level security: mTLS 1.3

On network level mutual TLS (mTLS) must be applied. The TLS-implementation must comply with the security level "Good" as specified by the National Cyber Security Centre (NCSC). At the time of writing, the current IT security guidelines for TLS require version 1.3 of the TLS standard for the security level "Good". The implementation of mTLS serves the following purposes:

- Authentication of client and server on network level
- Encryption of communication between client and server

The exchange of a client certificate during the mTLS handshake does not only enable the server to authenticate the client on network level, but it also enables the server to issue certificate bound access tokens as specified in RFC 8705 as an additional security measure on application level. See section Resource server authorization: OAuth 2.0 for requirements on application level security using OAuth 2.0.

Both the client and server certificates must be PKIo-certificates that are issued under the CA "Staat der Nederlanden Private Services CA – G1" (this includes UZI server certificates issued by UZI-registry (CIBG)).

Note that the requirements as specified in this paragraph apply to **Notification, FHIR, and token** endpoints.

3.2 Resource server authorization: OAuth 2.0

On application level both the Notification endpoint of the Receiving System and the FHIR endpoint of Sending System are considered as resource endpoints that must be secured by OAuth 2.0. This implies that a client that wants to interact with a resource server (FHIR or Notification endpoint) must obtain an access token from an authorization server before it can interact with that resource server. The client must present this access token as bearer token in the HTTP Authorization header of each request to the resource server as specified in RFC 6750 section 2.1.

3.2.1 Client authentication

The resource server must be able to authenticate the client as a trusted client. The client is specified as the **system** that submits the access token request (not to be confused with the **organization** for which that system is acting). The OAuth specs leave room for different authentication methods for client authentication. The authentication methods that are proposed in the OAuth 2.0 core specifications (RFC 6749 section 2.3) all rely on the exchange of shared secrets. The use of shared secrets is considered as a security risk since they are prone to leakage. The use of an authentication method that relies on digital signatures using asymmetric cryptography offers better security. Therefore, the client must authenticate itself by providing a client assertion by means of a signed JWT as specified in RFC 7523 section 2.2.

The client assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating system or to a third party trusted by the initiating system.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the client assertion. See RFC 7515 section 4.1.1. Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515 section 4.1.4.	Yes

The payload contains a set of claims listed below:

Claim	Description	Required
jti	Unique identifier of the client assertion. See RFC 7519 section 4.1.7.	Yes
iss	Identifier of the system that issued the client assertion. See RFC 7519 section 4.1.1 and RFC 7523 section 3.	Yes

Claim	Description	Required
iat	The time at which the client assertion was issued. See RFC 7519 section 4.1.6.	Conditional[5]
exp	The expiration time on or after which the client assertion shall not be accepted for processing. See RFC 7519 section 4.1.4 and RFC 7523 section 3.	Yes
nbf	The time before which the token shall not be accepted for processing. See RFC 7519 section 4.1.5 and RFC 7523 section 3.	No
aud	Identifier of the authorization server token endpoint where this client assertion is to be used. See RFC 7519 section 4.1.3 and RFC 7523 section 3. System vendors have to make mutual agreements about the value of this identifier.	Yes
sub	Identifier of the OAuth client that requests access. This claim must match the value of the client_id parameter in the access token request. Note that the client is specified as the system that submits the access token request. System vendors have to make mutual agreements about the value of this identifier.	Yes

The Issuer of the client assertion may include additional claims in the assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that was used to sign the client assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. Therefore, system vendors have to make mutual agreements about the exchange of these public keys.

Note that the authorization server can authenticate the client on network level by the client certificate that the client must present during the mTLS handshake (see section Network level security). In theory, this could be used by the authorization server to authenticate the client on application level. However, this may cause problems since it introduces additional and potentially unwanted requirements on TLS termination and related matters. Therefore, a client must always provide a client assertion in the access token request.

[5] If there is an agreed age of a client assertion.

3.2.2 Authorization grant

OAuth 2.0 requires the use of an authorization grant to request an access token. As specified in RFC 6749 section 1.3 “an authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token.” OAuth 2.0 specifies several different authorization grants. Additionally, there are several RFC’s that specify extension grants. Because this TA applies to situations where a resource client is acting on behalf of a user (health professional) that works for an organization (healthcare provider), the use of the JWT Bearer Assertion authorization grant as specified in RFC 7523 section 2.1 is the most suitable authorization grant. This means that the resource client must provide an authorization assertion in each access token request to identify the acting user, organization, and authorization base to prove that it is authorized to access the requested data. This authorization assertion acts as the authorization grant that the client can present to prove that it is authorized to access the protected resources.

The authorization assertion is a JWS Compact Serialized JWT that consists of a header, a payload, and a signature. The signature is created using a key pair belonging to the initiating organization or to a third party trusted by the initiating organization.

The header carries the claims listed below:

Claim	Description	Required
typ	Token type, must be “JWT”	Yes
alg	Cryptographic algorithm used to sign the authorization assertion. See RFC 7515 section 4.1.1. Must be one of PS256, PS384, PS512, ES256, ES384 or ES512.	Yes
kid	Identifier of the key pair used to sign this JWT. See RFC 7515 section 4.1.4.	Yes

The payload contains a set of claims that carry information required by NEN7512 and NEN7513.

Claim	Description	Required
jti	Unique identifier of the authorization assertion. See RFC 7519 section 4.1.7.	Yes
iss	Identifier of the system that issued the authorization assertion. See RFC 7519 section 4.1.1 and RFC 7523 section 3. System vendors have to make mutual agreements about the value of this identifier.	Yes
iat	The time at which the authorization assertion was issued. See RFC 7519 section 4.1.6.	Conditional[6]
exp	The expiration time on or after which the authorization assertion shall not be accepted for processing. See RFC 7519 section 4.1.4 and RFC 7523 section 3.	Yes

[6] The “iat” claim is only required if there is an agreed age of an authorization assertion.

Claim	Description	Required
nbf	The time before which the token shall not be accepted for processing. See RFC 7519 section 4.1.5 and RFC 7523 section 3.	No
aud	Identifier of the authorization server token endpoint where this authorization assertion is to be used. See RFC 7519 section 4.1.3 and RFC 7523 section 3.	Yes
sub	Identifier of the **organization** (healthcare supplier) that requests access. System vendors have to make mutual agreements about the value of this identifier.	Yes
user_id	Identifier of the **responsible user** (healthcare professional) who requests access. System vendors may make mutual agreements about the value of this identifier.	Conditional[7]
user_role	Code of the role of the responsible user (healthcare professional) who requests access. System vendors may make mutual agreements about the value of this identifier.	Conditional[8]
authorizer	Identifier of the **healthcare organization** that grants access. System vendors have to make mutual agreements about the value of this identifier.	Yes
authorization_base	See Authorization base	No
patient	Identifier of the patient for whom data is exchanged. Must be an OID encoded BSN (I.e., BSN with the “urn:oid:2.16.840.1.113883.2.4.6.3.” prefix and without a leading zero)	Conditional[9]

The Issuer of the authorization assertion may include additional claims in the authorization assertion, but the Issuer shall not require the authorization server to process these claims.

The exchange of the public key that was used to sign the authorization assertion between the Assertion Issuer and the authorization server is beyond the scope of this normative specification. Therefore, system vendors have to make mutual agreements about the exchange of these public keys.

[7] User identification (user_id and user_role claims) is only required in the authorization assertion when access to patient data is requested. This implies that these claims are not required in authorization assertions used in access token requests for Notification endpoints.

[8] See previous.

[9] Patient identification is only required when the Sending System requests access to the Notification endpoint of the Receiving System and the Sending System does not provide a Workflow Task that refers to a Patient resource containing the BSN of the patient. This way, the Receiving System is always able to identify a patient by BSN based on a Notification. The Receiving System must support receiving the BSN through the patient claim.

3.2.3 Authorization scope

The scope defines the requested access to the FHIR Server as specified in RFC 6749 section 3.3. If a scope is provided in the access token request or access token response, it must be expressed in a string of space delimited scopes as defined in SMART on FHIR v2. The following additional requirements apply to the scope values:

- When requesting an access token for a Notification endpoint at the Receiving System, the scope value must be one of:
    - `system/Task.c?code=http://fhir.nl/fhir/NamingSystem/TaskCode|pull-notification` (create)
    - `system/Task.u?code=http://fhir.nl/fhir/NamingSystem/TaskCode|pull-notification` (update)
- When requesting an access token for a FHIR endpoint at the Sending System, the query parameters in the scopes must match (a subset of) the queries in the FHIR search requests listed in Task.input of the Notification Task (see Notification message).

The client must provide the requested scope in the access token request, except for cases where an authorization base is provided in the access token request as part of the authorization assertion.

The authorization server must provide the granted access scope in the access token response in accordance with RFC 6749 section 5.1 and the requirements mentioned above. The issued access token must grant access to the granted scope that the authorization server specifies in the access token response. The granted scope must be equal to or less than the scope that can be derived from the authorization base consent token.

3.2.4 Access token request

Based on the paragraphs above each access token request contains the parameters listed below:

Parameter	Value	Required
grant_type	"urn:ietf:params:oauth:grant-type:jwt-bearer"	Yes
assertion	JWT authorization assertion as specified in paragraph Authorization grant.	
client_assertion_type	"urn:ietf:params:oauth:client-assertion-type:jwt-bearer"	Yes
client_assertion	JWT client assertion as specified in paragraph Client authentication.	Yes
client_id	ID of the resource client. This ID is issued by the authorization server. If present, the value of the "client_id" parameter must identify the same client as is identified by the client assertion.	No
scope	Space separated list of requested scopes, see paragraph Authorization scope.	Conditional

Note that the access token request effectively contains two JWT assertions:

1. A client assertion that is used to authenticate the client. This assertion identifies and authenticates the **system** that is requesting access.
2. An authorization assertion that is used as an authorization grant. This assertion identifies both the **organization** and **user** that are requesting access.

Separating client authentication from client authorization in two separate assertions enables the client to select different Assertion Issuers for the two assertions. The targeted authorization server must register both Issuers as trusted Assertion Issuers for a specific client.

3.2.5 Access token requirements

The access token will be processed only by the party that issued the access token. Therefore, the form and contents of the token are determined by the authorization server (audience), so the access token is opaque to the resource client. The resource client should not take any dependency on the format or contents of an access token. The authorization server MAY issue certificate bound access tokens as specified in RFC 8705, but this is not mandatory. To enable the server to issue certificate bound access tokens, the client MUST support mTLS for access token and resource requests as specified in section Network level security: mTLS 1.3.

3.3 Authorization base

When the Sending System receives a request from the Receiving System to access certain data, it is the primary responsibility of the Sending System to verify that the Receiving System is authorized to access that data. When publishing data on a resource server to be collected by the Receiving System, many Sending Systems register the authorization to access that data as an authorization base of some kind. To facilitate that authorization process, the Sending System may submit the authorization base (or a reference to it) to the Receiving System as part of the Notification (see section Notification message). If the Receiving System received an authorization base in the Notification, it must include that authorization base in the access token request to the Sending System (see section Authorization grant). This enables the authorization server of the Sending System to determine if the requested access can be granted based on the provided authorization base.

Since an authorization base is to be processed by the Sending System only, the form and contents of an authorization base are determined by the Sending System. The Receiving System should not take any dependency on the format or contents of an authorization base.

3.4 User authentication

Healthcare professionals are identified in their EHR system by logging in with their personal account. When a user of the Receiving System wants to request resources at the Sending System, the Sending System must be able to identify the user at the Receiving System as a legitimate healthcare professional who is working for the receiving organization before it can provide the requested data. Therefore, the Receiving System must implement the appropriate means to ensure the authenticity of the user.

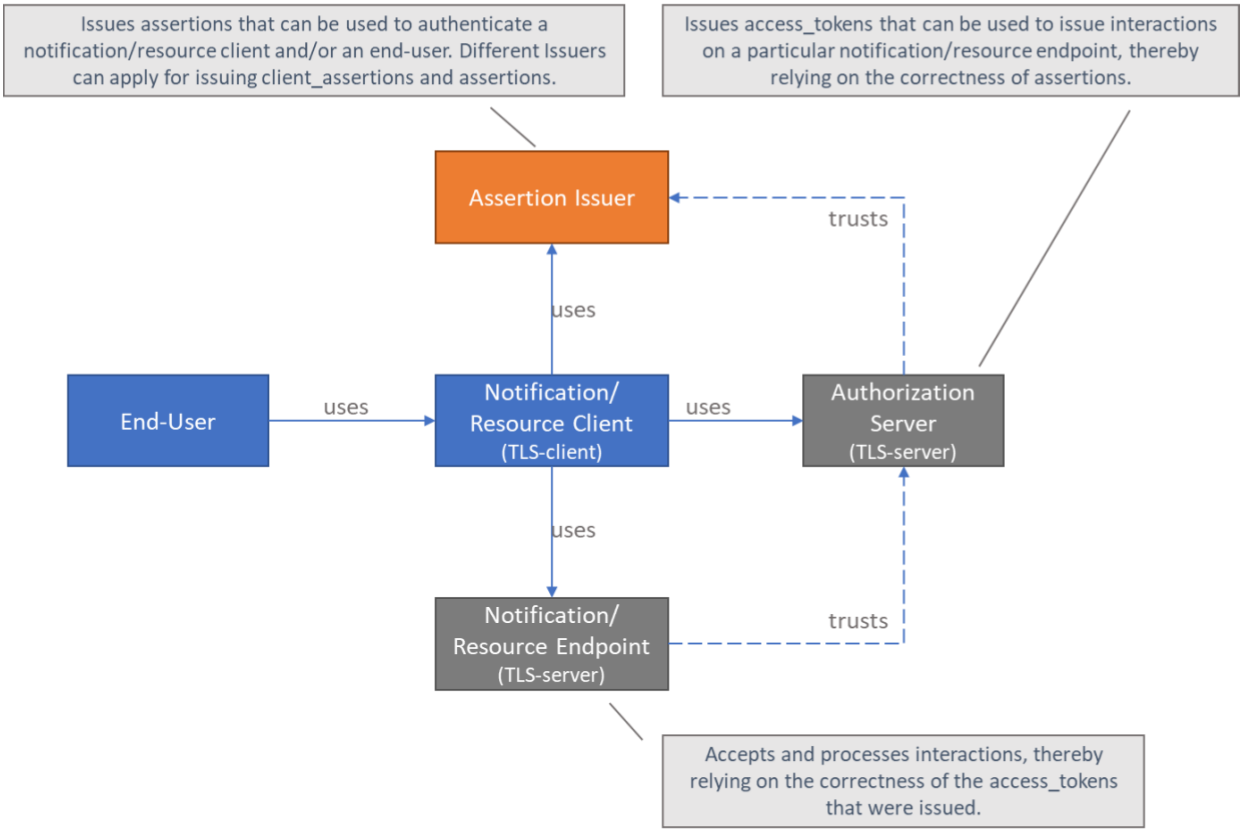
The Sending System can identify the healthcare professional at the receiving organization that is requesting patient data by the following claims in the authorization assertion of the access token request (see Authorization grant):

- **sub**: Identifier of the healthcare organization
- **user_id**: Identifier of the responsible user (healthcare professional)
- **user_role**: Code of the role of the responsible user (healthcare professional)

The type of identifiers used for organizations and users is beyond the scope of this TA. The same applies to the use of role codes.

3.5 Trust relationships

The picture below shows the different roles involved in the interactions, and clarifies the dependencies between these roles.


Issues assertions that can be used to authenticate a notification/resource client and/or an end-user. Different Issuers can apply for issuing client_assertions and assertions.
Issues access_tokens that can be used to issue interactions on a particular notification/resource endpoint, thereby relying on the correctness of assertions.
Assertion Issuer
trusts
uses
End-User
uses
Notification/ Resource Client (TLS-client)
uses
Authorization Server (TLS-server)
uses
Notification/ Resource Endpoint (TLS-server)
trusts
Accepts and processes interactions, thereby relying on the correctness of the access_tokens that were issued.

The Sending System hereby performs the following roles:

- Notification Client;
- Resource ServerEndpoint.

The Receiving System performs the roles:

- Notification ServerEndpoint;
- Resource Client.

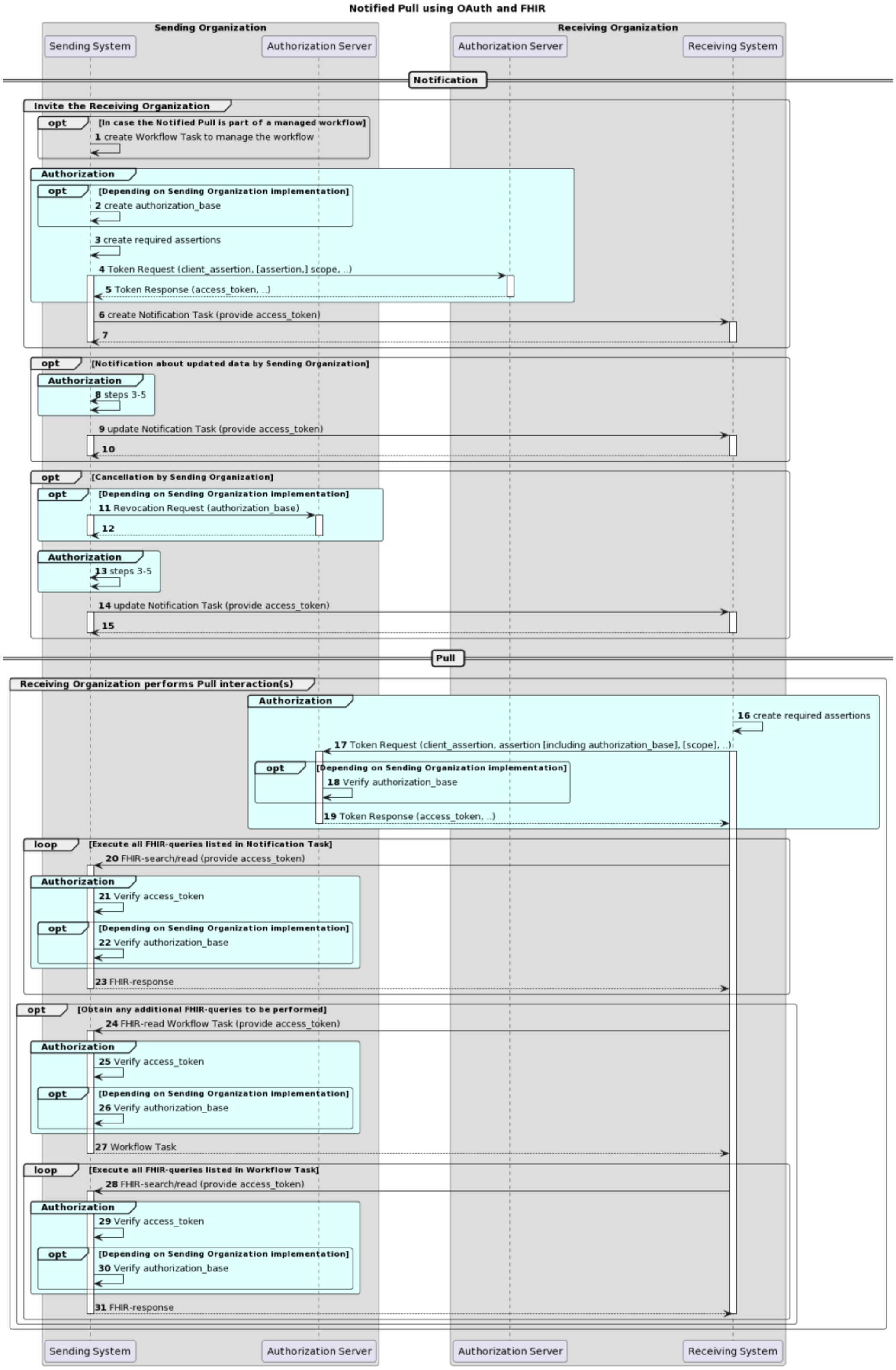
Sending System and Receiving System both implement the role of Authorization Server.

The role of Assertion Issuer can be performed by a third-party, but can also be performed by the Sending System or by the Receiving System. Assertion Issuers producing client assertions do not necessarily have to produce authorization assertions as well. Different Issuers can be used for these types of assertions. Before issuing an client assertion or an authorization assertion, the Assertion Issuer has to make sure that applicable requirements regarding user authentication and other mutual security agreements between the Sending System and Receiver System have been met.

Trust and required level of user authentication between parties has to be arranged and agreed upon prior to performing the interaction.

4 Full interaction sequence

The sequence diagram below visualizes the full flow for the Notified Pull interaction sequence including both interactions in the data layer using HL7 FHIR (described in chapter 2) and in authorization layer using OAuth 2.0 (marked cyan, described in chapter 3).


Notified Pull using OAuth and FHIR
Sending Organization
Receiving Organization
Sending System
Authorization Server
Authorization Server
Receiving System
Notification
Invite the Receiving Organization
opt
[In case the Notified Pull is part of a managed workflow]
1 create Workflow Task to manage the workflow
Authorization
opt
[Depending on Sending Organization implementation]
2 create authorization_base
3 create required assertions
4 Token Request (client_assertion, [assertion,] scope, ..)
5 Token Response (access_token, ..)
6 create Notification Task (provide access_token)
7
opt
[Notification about updated data by Sending Organization]
Authorization
8 steps 3-5
9 update Notification Task (provide access_token)
10
opt
[Cancellation by Sending Organization]
opt
[Depending on Sending Organization implementation]
11 Revocation Request (authorization_base)
12
Authorization
13 steps 3-5
14 update Notification Task (provide access_token)
15
Pull
Receiving Organization performs Pull interaction(s)
Authorization
16 create required assertions
17 Token Request (client_assertion, assertion [including authorization_base], [scope], ..)
opt
[Depending on Sending Organization implementation]
18 Verify authorization_base
19 Token Response (access_token, ..)
loop
[Execute all FHIR-queries listed in Notification Task]
20 FHIR-search/read (provide access_token)
Authorization
21 Verify access_token
opt
[Depending on Sending Organization implementation]
22 Verify authorization_base
23 FHIR-response
opt
[Obtain any additional FHIR-queries to be performed]
24 FHIR-read Workflow Task (provide access_token)
Authorization
25 Verify access_token
opt
[Depending on Sending Organization implementation]
26 Verify authorization_base
27 Workflow Task
loop
[Execute all FHIR-queries listed in Workflow Task]
28 FHIR-search/read (provide access_token)
Authorization
29 Verify access_token
opt
[Depending on Sending Organization implementation]
30 Verify authorization_base
31 FHIR-response
Sending System
Authorization Server
Authorization Server
Receiving System

The flow contains the following sections:

- Invite the Receiving System;
- Notification about updated data by Sending Organization (option), this block is only required when the Sending Organization needs to notify the Receiving Organization about data having been updated at the Sending Organization;
- Cancellation by Sending Organization (option), this block is only to be used when the Sending Organization needs to withdraw the Pull invitation, e.g., when the Sending Organization invited a wrong Receiving Organization;
- Receiving System performs Pull interaction(s).

Each section consists of several steps. The steps correspond to the numbers in the sequence diagram.

Section	Step	Description
Invite the Receiving Organization	1	If the Notified Pull is part of a managed workflow involving both the Sending Organization and the Receiving Organization, and this workflow specifies the creation of a FHIR Task “Workflow Task” at the Sending System, then the flow starts with a creation of this Task on the Sending System.
	2	The Sending System creates an authorization base, which is used later to communicate a presumed consent for the exchange of patient information. The Receiving System must treat the authorization base as an opaque element. The Receiving System should not depend on any information contained in the authorization base.
	3	The Sending System creates one or two assertions, which can be used to request an access token in the next step.
	4-5	The Sending System requests an access token which can be used in step 6. The Receiving System processes the token request and returns a token response containing (among others) an access token. The Sending System must treat the access token as opaque. The Sending System should not depend on any information contained in the access token.
	6-7	By invoking a create interaction regarding a FHIR Task (“Notification Task”) on the Receiving System, the Sending System invites the Receiving System to perform one or more Pull interactions. The Receiving System processes the invitation and sends a technical response to complete the create interaction.
Notification about updated data by Sending Organization	8	The Sending System repeats steps 3-5.
	9-10	The Sending System updates the Notification Task on the Receiving System. The Receiving System returns a technical response message.
Cancellation by Sending Organization	11-12	The “Cancellation by Sending Organization” option provides a means for the Sending System to cancel/revoke an erroneously created Notification. Depending on the implementation at the Sending Organization, the Sending System might have to start the cancellation by revoking the authorization base created in step 2, by sending a revocation request to the Sending Organization’s Authorization Server. The Authorization Server processes the request and returns a response.
	13	The Sending System repeats steps 3-5.
	14-15	The Sending Organization informs the Receiving Organization by updating the Notification Task on the Receiving System (Task.status is set to “cancelled”). The Receiving System returns a technical response message.
	16	The Receiving System creates one or two assertions, which can be used to request an access token in the next step.

Section	Step	Description
Receiving Organization performs Pull interaction(s)	17-19	The Receiving System requests an access token which can be used to perform the intended Pull interactions. The Sending Organization’s Authorization Server processes the token request and returns a token response containing (among others) an access token. Depending on the Sending System implementation, the Sending System can choose to verify the consent before issuing an access token (preferred option). The Receiving System must treat the access token as an opaque element. The Receiving System should not depend on any information contained in the access token.
	20-23	The Receiving System initiates the intended interactions and processes the responses. The Sending System verifies the access token and can additionally decide to verify the authorization base at this point in the flow.
	24-27	In case the Notification Task indicates that a Workflow Task is available that contains (additional) Pull interactions to be performed, the Receiving System obtains this Workflow Task from the Sending System.
	28-31	The Receiving System initiates the (additional) Pull interactions listed in the Workflow Task, and processes the responses.

5 Identification and addressing

Please note: This chapter is not normative but informative.

Every connected healthcare organization has at least three endpoints that should be known by another organization:

- Notification endpoint; the endpoint to which the Notification can be pushed
- Authorization server token endpoint; the endpoint where the access token can be requested.
- Resource server endpoint; the endpoint which is used to request the actual resources.

Endpoints can be used for multiple organizations. The identification of the Sending Organization will be managed in the Notification. An Identifier that is used for an Organization should be an URI. For example with the code system OID, DID[10] or (Dutch) URA.

To achieve specific delivery for automatic processing within a Receiving Organization or internal routing to a specific internal user of the Receiving Organization additional agreements will be made. Agreements about this topic will be specified in the specific use-case for now.

Communication/publication of the endpoints and identifiers of each organization will be managed outside this Technical Agreement between implementing partners, or so-called trusted gateways/nodes/trusted networks. So, the exact method of distribution of endpoint URLs is not specified in this version of the TA.

Options:

- Using a trusted third party that acts as an Issuer of endpoint information (e.g., "ZORG-AB")
- Using a distributed registry that is managed by the connected healthcare organizations and/or their system
- Using mutual agreements between integrationImplementing partners have made an agreement about their own communication method for endpoints and organizations

There are several methods to share endpoint URLs, via another endpoint URL of a connected healthcare organization:

- Share Authorization server endpoint via the Resource Server's SMART configuration:
  - Via /.well-known/smart-configuration
  - https://build.fhir.org/ig/HL7/smart-app-launch/conformance.html
- Share Resource Server endpoint via the Authorization Server's well-known registry
  - https://rwww.rfc-editor.org/rfc/rfc8414.html#section-7.3

[10] More information about DID: https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers

6 Document management

6.1 Involved parties

495 This document is a co-creation of the companies listed below. The following people have been involved in creating this document.

Company	Contact person	Mail
Chipsoft	Vincent van den Berg	v.van.den.berg@chipsoft.com
Nexus	Dennis Willemsen	dennis.willemsen@nexus-nederland.nl
Tenzinger	Jorrit Spee	jorrit@jorritspee.nl
Twiin	Marc Sandberg	marc.sandberg@vzvz.nl
VZVZ	Ron van Holland	ron.van.holland@vzvz.nl
ZorgDomein	Stephan Opdenberg	opdenberg@zorgdomein.nl
ZorgDomein	Ruben Pape	pape@zorgdomein.nl

6.2 Version control

Rev	Release Date	Author	Description of change
0.9	23-01-2023	All	Version for consultation
0.99	04-05-2023	All	Version for publication Updates based on the feedback following the consultation.

Appendix: Examples

Token Request

request

```
POST /receiver-auth-server/token
Host: sending-server.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
assertion=ew0KICAidHlwIjogIkp[...omitted for brevity...]
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-
bearer
client_assertion=ew0KICAidHlwIjogIkp[...omitted for brevity...]
```

client_assertion jwt payload

```
{
 "jti": "4f0dfb37-7f9d-45fa-8187-9e260b80f949",
 "iss": "sending-ehr-issuer-id",
 "iat": "1572468316",
 "exp": "1572468916",
 "aud": "auth-server-id",
 "sub": "sending-ehr-system-id"
}
```

assertion jwt payload

```
{
 "jti": "4f0dfb37-7f9d-45fa-8187-9e260b80f949",
 "iss": "sending-ehr-issuer-id",
 "iat": "1572468316",
 "exp": "1572468916",
 "aud": "auth-server-id",
 "sub": "sending-organization-id",
 "user_id": "responsible-user-id",
 "user_role": "responsible-user-role",
 "authorizer": "receiving-organization-id",
 "authorization_base": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2",
 "patient": "urn:oid:2.16.840.1.113883.2.4.6.3.123456782"
}
```

Notification Task

New Notification Task

```
{
  "resourceType": "Task",
  "groupIdentifier": {
    "system": "https://tools.ietf.org/html/rfc4122",
    "value": "urn:uuid:484639e6-e647-464c-8722-6e8a73cda4e0"
  },
  "identifier": {
    "system": "https://tools.ietf.org/html/rfc4122",
    "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
  },
  "status": "requested",
  "intent": "proposal",
  "code": {
    "coding": [
      {
        "system": "http://fhir.nl/fhir/NamingSystem/TaskCode",
        "code": "pull-notification"
      }
    ]
  },
  "restriction": {
    "period": {
      "end": "2023-10-14T15:36:05+02:00"
    }
  },
  "for": {
    "identifier": {
      "system": "http://fhir.nl/fhir/NamingSystem/bsn",
      "value": "172642863"
    }
  },
  "authoredOn": "2023-04-13T15:01:54+02:00",
  "requester": {
    "agent": {
      "identifier": {
        "system": "http://example.com/fhir/NamingSystem/dummy",
        "value": "sending-ehr-system-id"
      }
    },
    "onBehalfOf": {
      "identifier": {
        "system": "http://example.com/fhir/NamingSystem/dummy",
        "value": "sending-organization-id"
      }
    }
  },
  "owner": {
    "identifier": {
      "system": "http://example.com/fhir/NamingSystem/dummy",
      "value": "receiving-organization-id"
    }
  },
  "input": [
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.nl/fhir/NamingSystem/TaskParameter",
            "code": "authorization-base"
          }
        ]
      },
      "value": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.nl/fhir/NamingSystem/TaskParameter",
            "code": "read-resource",
            "display": "Laboratory test"
          }
        ]
      },
      "valueReference": {
        "reference": "Observation/123456"
      }
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "77599-9",
           "display": "Additional documentation"
         }
       ]
     },
     "valueString": "DocumentReference?status=current"
   }
 ]
}
```

Cancel Notification Task

```
{
 "resourceType": "Task",
 "identifier": {
   "system": "https://tools.ietf.org/html/rfc4122",
   "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
 },
 "status": "cancelled",
 "intent": "proposal"
}
```

New Notification Task for BgZ including Additional documentation

```
{
 "resourceType": "Task",
 "groupIdentifier": {
   "system": "https://tools.ietf.org/html/rfc4122",
   "value": "urn:uuid:484639e6-e647-464c-8722-6e8a73cda4e0"
 },
 "identifier": {
   "system": "https://tools.ietf.org/html/rfc4122",
   "value": "urn:uuid:6128cfe7-0e89-4d37-ba90-e4ca3b3fcbbe"
 },
 "status": "requested",
 "intent": "proposal",
 "code": {
   "coding": [
     {
       "system": "http://fhir.nl/fhir/NamingSystem/TaskCode",
       "code": "pull-notification"
     }
   ]
 },
 "restriction": {
   "period": {
      "end": "2023-10-14T15:36:05+02:00"
    }
  },
  "for": {
    "identifier": {
      "system": "http://fhir.nl/fhir/NamingSystem/bsn",
      "value": "172642863"
    }
  },
  "authoredOn": "2023-04-13T15:01:54+02:00",
  "requester": {
    "agent": {
      "identifier": {
        "system": "http://example.com/fhir/NamingSystem/dummy",
        "value": "sending-ehr-system-id"
      }
    },
    "onBehalfOf": {
      "identifier": {
        "system": "http://example.com/fhir/NamingSystem/dummy",
        "value": "sending-organization-id"
      }
    }
  },
  "owner": {
    "identifier": {
      "system": "http://example.com/fhir/NamingSystem/dummy",
      "value": "receiving-organization-id"
    }
  },
  "input": [
    {
      "type": {
        "coding": [
          {
            "system": "http://fhir.nl/fhir/NamingSystem/TaskParameter",
            "code": "authorization-base"
          }
        ]
      },
      "value": "ZGFhNDFjY2MtZGFmMi00YjZkLThiNDYtN2JlZDk1MWEyYzk2"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "79191-3",
            "display": "Patient demographics panel"
          }
        ]
      },
      "valueString": "Patient?_include=Patient:general-practitioner"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "48768-6",
            "display": "Payment sources Document"
          }
        ]
      },
      "valueString":
"Coverage?_include=Coverage:payor:Organization&_include=Coverage:payor:Patient"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "11291000146105",
            "display": "Treatment instructions"
          }
        ]
      },
      "valueString": "Consent?category=http://snomed.info/sct|11291000146105"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "11341000146107",
            "display": "Living will and advance directive record"
          }
        ]
      },
      "valueString": "Consent?category=http://snomed.info/sct|11341000146107"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "47420-5",
            "display": "Functional status assessment note"
          }
        ]
      },
      "valueString":
"Observation/$lastn?category=http://snomed.info/sct|118228005,http://snomed.info/
sct|384821006"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "11450-4",
            "display": "Problem list - Reported"
          }
        ]
      },
      "valueString": "Condition"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "365508006",
            "display": "Residence and accommodation circumstances - finding"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://snomed.info/sct|365508006"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "228366006",
            "display": "Finding relating to drug misuse behavior"
          }
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|228366006"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "228273003",
            "display": "Finding relating to alcohol drinking behavior"
          }
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|228273003"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "365980008",
            "display": "Tobacco use and exposure - finding"
          }
        ]
      },
      "valueString": "Observation?code=http://snomed.info/sct|365980008"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "11816003",
            "display": "Diet education"
          }
        ]
      },
      "valueString": "NutritionOrder"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "75310-3",
            "display": "Health concerns Document"
          }
        ]
      },
      "valueString": "Flag"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "48765-2",
            "display": "Allergies and adverse reactions Document"
          }
        ]
      },
      "valueString": "AllergyIntolerance"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "422979000",
            "display": "Known medication use"
          }
        ]
      },
      "valueString":
"MedicationStatement?category=urn:oid:2.16.840.1.113883.2.4.3.11.60.20.77.5.3|6&_
include=MedicationStatement:medication"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "16076005",
            "display": "Known medication agreements"
          }
        ]
      },
      "valueString":
"MedicationRequest?category=http://snomed.info/sct|16076005&_include=MedicationRe
quest:medication"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "422037009",
            "display": "Known administration agreements"
          }
        ]
      },
      "valueString":
"MedicationDispense?category=http://snomed.info/sct|422037009&_include=Medication
Dispense:medication"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "46264-8",
            "display": "Known medical aids"
          }
        ]
      },
      "valueString": "DeviceUseStatement?_include=DeviceUseStatement:device"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "11369-6",
            "display": "History of Immunization Narrative"
          }
        ]
      },
      "valueString": "Immunization?status=completed"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "85354-9",
            "display": "Blood pressure"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|85354-9"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "29463-7",
            "display": "Body weight"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|29463-7"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "8302-2",
            "display": "Body height"
          }
        ]
      },
      "valueString": "Observation/$lastn?code=http://loinc.org|8302-
2,http://loinc.org|8306-3,http://loinc.org|8308-9"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://snomed.info/sct",
            "code": "15220000",
            "display": "Laboratory test"
          }
        ]
      },
      "valueString":
"Observation/$lastn?category=http://snomed.info/sct|275711006&_include=Observation:related-target&_include=Observation:specimen"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "47519-4",
            "display": "History of Procedures"
          }
        ]
      },
      "valueString": "Procedure?category=http://snomed.info/sct|387713003"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "46240-8",
            "display": "History of Hospitalizations+Outpatient visits Narrative"
          }
        ]
      },
      "valueString":
"Encounter?class=http://hl7.org/fhir/v3/ActCode|IMP,http://hl7.org/fhir/v3/ActCode|ACUTE,http://hl7.org/fhir/v3/ActCode|NONAC"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "18776-5",
            "display": "Plan of care note"
          }
        ]
      },
      "valueString": "ProcedureRequest?status=active"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "18776-5",
            "display": "Plan of care note"
          }
        ]
      },
      "valueString": "ImmunizationRecommendation"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "18776-5",
            "display": "Plan of care note"
          }
        ]
      },
      "valueString": "DeviceRequest?status=active&_include=DeviceRequest:device"
    },
    {
      "type": {
        "coding": [
          {
            "system": "http://loinc.org",
            "code": "18776-5",
            "display": "Plan of care note"
          }
        ]
      },
      "valueString": "Appointment?status=booked,pending,proposed"
    },
    {
      "type": {
        "coding": [
          {
           "system": "http://loinc.org",
           "code": "77599-9",
           "display": "Additional documentation"
         }
       ]
     },
     "valueString": "DocumentReference?status=current"
   }
 ]
}
```

Appendix: BgZ implementation

The implementation for BgZ with Notified Pull is fully based on the Nictiz information standard “BgZ medisch specialistische zorg”, which itself is based on the MedMij BgZ. This appendix will provide a guideline on how to use the Notified Pull exchange pattern to transfer the BgZ between two healthcare organizations.

The Sending System may choose to provide a Workflow Task resource that can be used to exchange status updates and other workflow related details related to the healthcare process that demands the data exchange. In the context of a BgZ-referral, the Sending System may choose to provide a Workflow Task resource that is used to exchange details about status updates or other workflow updates related to the referral (see Notification scope).

An example of a BgZ Workflow Task profile

Name	Card.	Type	Comments
definition	0..1	Reference(ActivityDefinition)	Reference to ActivityDefinition resources that defines the requested activity or service
status	1..1	code	requested | received | accepted | rejected | cancelled | completed
intent	1..1	code	“order”
priority	0..1	code	normal | urgent | asap | stat
code	1..1	CodeableConcept	
-- coding	1..1	Coding	
-- -- SNOMED	1..1	Slice	
-- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- code	1..1	code	“3457005”
-- -- -- display	0..1	string	“verwijzen van patiënt”
-- text	1..1	string	“Verwijzing”
description	0..1	string	
focus	0..1	Reference(ReferralRequest | CarePlan)	
for	0..1	Reference(nl-core-patient)	Reference to referred patient
authoredOn	0..1	dateTime	Date of referral submission
requester	0..1	BackboneElement	
-- agent	1..1	Reference(nl-core-practitioner)	Reference to the practitioner who sent the referral
-- -- extension		Extension	
-- -- -- practitionerRole		Extension(Reference(nl-core-practitionerrole))	Extension to relate the Practitioner to an organization, Location, HealthcareService, role, specialism, etc.
-- onBehalfOf	0..1	Reference(nl-core-organization)	Reference to the Sending Organization
owner	0..1	Reference(nl-core-organization)	Reference to the Receiving Organization
restriction	0..1	BackboneElement	
-- period	0..1	Period	
-- -- start	0..1	dateTime	Earliest date to start requested treatment or service
-- -- end	0..1	dateTime	Latest date to start requested treatment or service
input	0..*	BackboneElement	

Name	Card.	Type	Comments
-- patientInformation	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“79191-3”
-- -- -- -- display	0..1	string	“Patient demographics panel”
-- -- text	1..1	string	“Patient information”
-- -- valueString	1..1	string	“/Patient?_include=Patient:general-practitioner”
-- paymentDetails	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“48768-6”
-- -- -- -- display	0..1	string	“Payment sources”
-- -- text	1..1	string	“Insurance information”
-- -- valueString	1..1	string	“/Coverage?_include=Coverage:payor:Patient&_include=Coverage:payor:Organization”
-- treatmentDirective	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11291000146105”
-- -- -- -- display	0..1	string	“Treatment instructions”
-- -- text	1..1	string	“Known treatment directives”
-- -- valueString	1..1	string	“/Consent?category=http://snomed.info/sct|11291000146105”
-- advanceDirective	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11341000146107”
-- -- -- -- display	0..1	string	“Living will and advance directive record”
-- -- text	1..1	string	“Known advance directives”
-- -- valueString	1..1	string	“/Consent?category=http://snomed.info/sct|11341000146107”
-- functionalStatus	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”

Name	Card.	Type	Comments
-- -- -- -- code	1..1	code	“47420-5”
-- -- -- -- display	0..1	string	“Functional status assessment note”
-- -- text	1..1	string	“Last known functional / mental status”
-- -- valueString	1..1	string	“/Observation/$lastn?category=http://snomed.info/sct|118228005,http://snomed.info/sct|384821006”
-- problems	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11450-4”
-- -- -- -- display	0..1	string	“Problem list”
-- -- text	1..1	string	“All known problems”
-- -- valueString	1..1	string	“/Condition”
-- livingSituation	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“365508006”
-- -- -- -- display	0..1	string	“Finding of residence and accommodation circumstances”
-- -- text	1..1	string	“Current living situation”
-- -- valueString	1..1	string	“/Observation/$lastn?code=http://snomed.info/sct|365508006”
-- drugUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“228366006”
-- -- -- -- display	0..1	string	“Finding relating to drug misuse behavior”
-- -- text	1..1	string	“All known drug use”
-- -- valueString	1..1	string	“/Observation?code=http://snomed.info/sct|228366006”
-- alcoholUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“228273003”
-- -- -- -- display	0..1	string	“Finding relating to alcohol drinking behavior”
-- -- text	1..1	string	“All known alcohol use”
-- -- valueString	1..1	string	“/Observation?code=http://snomed.info/sct|228273003”

Name	Card.	Type	Comments
-- tobaccoUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“365980008”
-- -- -- -- display	0..1	string	“Finding of tobacco use and exposure”
-- -- text	1..1	string	“All known tobacco use”
-- -- valueString	1..1	string	“/Observation?code=http://snomed.info/sct|365980008”
-- nutritionAdvice	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“11816003”
-- -- -- -- display	0..1	string	“Diet education”
-- -- text	1..1	string	“All known dietary recommendations”
-- -- valueString	1..1	string	“/NutritionOrder”
-- alert	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“75310-3”
-- -- -- -- display	0..1	string	“Health concerns”
-- -- text	1..1	string	“All known alerts”
-- -- valueString	1..1	string	“/Flag”
-- allergyIntolerance	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“48765-2”
-- -- -- -- display	0..1	string	“Allergies and adverse reactions”
-- -- text	1..1	string	“All known information regarding allergies”
-- -- valueString	1..1	string	“/AllergyIntolerance”
-- medicationUse	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“16076005”
-- -- -- -- display	0..1	string	“Prescription”

Name	Card.	Type	Comments
-- -- text	1..1	string	“Known medication use”
-- -- valueString	1..1	string	“/MedicationStatement?category=urn:oid:2.16.840.1.113883.2.4.3.11.60.20.77.5.3|6&_include=MedicationStatement:medication”
-- medicationAgreement	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“422037009”
-- -- -- -- display	0..1	string	“Provider medication administration instructions”
-- -- text	1..1	string	“Known medication agreements”
-- -- valueString	1..1	string	“/MedicationRequest?category=http://snomed.info/sct|16076005&_include=MedicationRequest:medication”
– administrationAgreement	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	“http://snomed.info/sct”
-- -- -- -- code	1..1	code	“422979000”
-- -- -- -- display	0..1	string	“Medication regimen behavior finding”
-- -- text	1..1	string	“Known administration agreements”
-- -- valueString	1..1	string	“/MedicationDispense?category=http://snomed.info/sct|422037009&_include=MedicationDispense:medication”
-- medicalAids	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“46264-8”
-- -- -- -- display	0..1	string	“History of medical device use”
-- -- text	1..1	string	“Known medical aids”
-- -- valueString	1..1	string	“/DeviceUseStatement?_include=DeviceUseStatement:device”
-- vaccinations	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“11369-6”
-- -- -- -- display	0..1	string	“Immunization”
-- -- text	1..1	string	“Known vaccinations”
-- -- valueString	1..1	string	“/Immunization?status=completed”
-- bloodPressure	0..1	Slice	

Name	Card.	Type	Comments
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	"http://loinc.org"
-- -- -- -- code	1..1	code	"85354-9"
-- -- -- -- display	0..1	string	"Blood pressure panel"
-- -- text	1..1	string	"Last known blood pressure"
-- -- valueString	1..1	string	"/Observation/$lastn?code=http://loinc.org|85354-9"
-- bodyWeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	"http://loinc.org"
-- -- -- -- code	1..1	code	"29463-7"
-- -- -- -- display	0..1	string	"Body weight"
-- -- text	1..1	string	"Last known body weight"
-- -- valueString	1..1	string	"/Observation/$lastn?code=http://loinc.org|29463-7"
-- bodyHeight	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	"http://loinc.org"
-- -- -- -- code	1..1	code	"8302-2"
-- -- -- -- display	0..1	string	"Body height"
-- -- text	1..1	string	"Last known body height"
-- -- valueString	1..1	string	"/Observation/$lastn?code=http://loinc.org|8302-2,http://loinc.org|8306-3,http://loinc.org|8308-9"
-- results	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- SNOMED	1..1	Slice	
-- -- -- -- system	1..1	string	"http://snomed.info/sct"
-- -- -- -- code	1..1	code	"15220000"
-- -- -- -- display	0..1	string	"Laboratory test"
-- -- text	1..1	string	"Last known laboratory results per type"
-- -- valueString	1..1	string	"/Observation/$lastn?category=http://snomed.info/sct|275711006&_include=Observation:related-target&_include=Observation:specimen"
-- procedures	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	"http://loinc.org"

Name	Card.	Type	Comments
-- -- -- -- code	1..1	code	“47519-4”
-- -- -- -- display	0..1	string	“History of procedures”
-- -- text	1..1	string	“Known surgical procedures”
-- -- valueString	1..1	string	“/Procedure?category=http://snomed.info/sct|387713003”
-- encounters	0..1	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“46240-8”
-- -- -- -- display	0..1	string	“Hospitalizations+Outpatient visits”
-- -- text	1..1	string	“Known hospital admissions (no outpatient contacts)”
-- -- valueString	1..1	string	“/Encounter?class=http://hl7.org/fhir/v3/ActCode|IMP,http://hl7.org/fhir/v3/ActCode|ACUTE,http://hl7.org/fhir/v3/ActCode|NONAC”
-- plannedCare	0..4	Slice	
-- -- type	1..1	CodeableConcept	
-- -- coding	1..*	Coding	
-- -- -- LOINC	1..1	Slice	
-- -- -- -- system	1..1	string	“http://loinc.org”
-- -- -- -- code	1..1	code	“18776-5”
-- -- -- -- display	0..1	string	“Plan of care note”
-- -- text	1..1	string	“Known planned care activities”
-- -- valueString	1..1	string	“/ProcedureRequest?status=active” or “/ImmunizationRecommendation” or “/DeviceRequest?status=active&_include=DeviceRequest:device” or “/Appointment?status=booked,pending,proposed”

525 As described in the section Notified Pull interaction every reference can be coded specific to the part. The codes of all HCIMs are in the table below.

HCIM	Code	System
Patient **MaritalStatus** **ContactPerson** **HealthProfessional**	79191-3	http://loinc.org
Payer	48768-6	http://loinc.org
TreatmentDirective	11291000146105	http://snomed.info/sct
AdvanceDirective	11341000146107	http://snomed.info/sct
FunctionalOrMentalStatus	47420-5	http://loinc.org
Problem	11450-4	http://loinc.org

LivingSituation	365508006	http://snomed.info/sct
DrugUse	228366006	http://snomed.info/sct
AlcoholUse	228273003	http://snomed.info/sct
TobaccoUse	365980008	http://snomed.info/sct
NutritionAdvice	11816003	http://snomed.info/sct
Alert	75310-3	http://loinc.org
AllergyIntolerance	48765-2	http://loinc.org
MedicationAgreement	16076005	http://snomed.info/sct
AdministrationAgreement	422037009	http://snomed.info/sct
MedicationUse2	422979000	http://snomed.info/sct
MedicalDevice	46264-8	http://loinc.org
Vaccination	11369-6	http://loinc.org
BloodPressure	85354-9	http://loinc.org
BodyWeight	29463-7	http://loinc.org
BodyHeight	8302-2	http://loinc.org
LaboratoryTestResult	15220000	http://snomed.info/sct
Procedure	47519-4	http://loinc.org
Encounter	46240-8	http://loinc.org
PlannedCareActivityForTransfer	18776-5	http://loinc.org

Appendix: Notification considerations

In the process of deciding the content of the Notification several options have been up for review. This appendix has been added to inform about the options that were reviewed, and to a certain extent why they were ultimately not used.

Resource	Pros / cons	Deciding factor
Bundle type Collection	● Communication of a (collection of) resource(s) is usually done using a Bundle, because of its flexibility. ● Light weight; this type forces minimalization of data. This way only clinical data can be transmitted. ● Suits the narrative when changing to R5 alternatives. ● Extensible with entry.link, to add more detail about the send resources.	The suggestion was made to not include the resources itself in this resource. But the collection explicitly needs the entry to contain the resource itself.
List	● Easy solution, conceptually ready for Notification. ● No support for search queries. ● No support for linked request resources. ● No real support for details on Sending Organization and/or Receiving Organization.	Too many cons, which should really be supported for Notification purposes.
AuditEvent	● A lot of space to go into detail about which data is made available for what party. ● Limited support for search queries. ● No support for linked request resources. ● No support for recipient details.	Purpose-build for auditing specific actions, not as a Notification.
Consent	● Support for an end-date. ● Links a Notification to the authorization, while authorization should be concluded from the consent or access token. ● No support for search queries. ● No support for linked request resources. ● No real support for details on Sending Organization and/or Receiving Organization.	Purpose-build to contain consent, not a Notification. Would insinuate availability based on resource, while consent and access token are still needed to determine authorization.