

UC-118-Put Consent-HC Org-HIO

Used Documentation

Cookbook / Materials	Version	Location
Consent WS	1.9	https://www.ehealth.fgov.be/ehealthplatform/nl/service-ehealthconsent

General info

Informed Consent

The existence of an active 'informed patient consent' is one of the fundamental prerequisites for the healthcare providers to access patient's medical data. Therefore, the eHealth platform makes available to the concerned patients and the health care actors involved in the exchange, storage or referencing personal data a service to manage the 'informed patient consent' as defined by the deliberation 12/047 of the CSSSS /SCSZG1.

Technically, we identify the following attributes for an 'informed patient consent':

- The SSIN of the patient.
- The date of the consent registration (at the end-user side).
- The "type" of the consent If the consent is only valuable for data posterior to the signing date, it is called 'prospective' and 'retrospective' in the other case . According to the rules defined now, the only possible value for this attribute is 'retrospective'. The attribute is present for backwards compatibility.
- The identity of the HCParty acting in the patient's name (if applicable).

KMEHR


This service is a 'KMEHR-based' WS. We thus strongly recommend consulting the documentation related to the KMEHR normative elements. The KMEHR site aims to offer a central point for the documentation of the KMEHR normative elements.

<https://www.ehealth.fgov.be/standards/kmehr/en>

The three following generic elements are, in particular, essentials to build the request and the reply of eHealth Consent WS.


- **cd** : This is the key element used to code information: this section is completely based on the description from the KMEHR standard, as can be found on: <https://www.ehealth.fgov.be/standards/kmehr/en/page/key-elements#cd>
- **id**: This element is used to uniquely identify key elements like request, response of the WS, patient, HCParty. It can also be used to specify any unique identifier: this section is completely based on the description from the KMEHR standard, as can be found on: <https://www.ehealth.fgov.be/standards/kmehr/en/page/key-elements#id>
- **HC Party**: The hcparty element is a generic element that aims to represent any kind of healthcare party: organization, physician, medical specialty, or even IT systems: this section is entirely based on the description from the KMEHR standard, as can be found on: <https://www.ehealth.fgov.be/standards/kmehr/en/page/hcparty>

Basic Flow

Flow	Specifications						
 Unknown macro: 'drawio'	<table><tr><td>ID</td><td>UC-118-BF</td></tr><tr><td>Name</td><td>Put Patient Consent - HC Organization -Health Insurance Organisation - Doctor</td></tr><tr><td>Description</td><td>A doctor working in the concerned Health Insurance Organization (HIO) declares an Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS.</td></tr></table>	ID	UC-118-BF	Name	Put Patient Consent - HC Organization - Health Insurance Organisation - Doctor	Description	A doctor working in the concerned Health Insurance Organization (HIO) declares an Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS.
ID	UC-118-BF						
Name	Put Patient Consent - HC Organization - Health Insurance Organisation - Doctor						
Description	A doctor working in the concerned Health Insurance Organization (HIO) declares an Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS.						

Actor (s)	A doctor working in the concerned HIO
Requirements	<ul style="list-style-type: none"> • End-user is a doctor working in the concerned HIO • Valid eHealth Certificate of the HIO • Consent WS is integrated in the software of the end-user • The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software • Identification of the HIO: CBE number, HIO category • Identification of the doctor: SSIN number, NIHI (if available), the professional category • Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p>
Trigger	The user wants to declare a Patient Consent on behalf of the patient
Precondition (s)	<ul style="list-style-type: none"> • The user has an account for the application • The user is logged out
Flow	<ol style="list-style-type: none"> 1. The user attempts to access the eHealth Consent WS 2. The user needs to request a SAML Token by using his eID 3. A request for a SAML Token is sent to the Secure Token Service (STS) 4. The STS responds with a SAML Token 5. The user has access to the eHealth WS Consent 6. The user does a request for Put Patient Consent 7. The Put Patient Consent Request is sent to the WS Consent 8. The informed Patient Consent is stored in eHealth Database 9. The request is logged 10. The WS Consent responds with a Put patient consent response
Post condition(s)	<ul style="list-style-type: none"> • Request is logged • Informed Patient Consent is stored in the eHealth Database
Test Data	<ul style="list-style-type: none"> • Example Request HIO - Doctor • Example PutPatientConsentRequest • Example PutPatientConsentResponse
Endpoint(s)	<ul style="list-style-type: none"> • WS Consent • eHealth Database
Remarks	<ul style="list-style-type: none"> • If support card number is provided then it must be compliant e.g. correct format, check-digit and combination • Support card number is not mandatory if the concerned patient is a new born (0 < patient < 3 months)
Additional Information	Additional information about the HIO, doctor e.g. software name, address, doctor name may be added for the audit purpose

Alternative Flow

Flow	Specifications																						
 Unknown macro: 'drawio'	<table> <tr> <td>ID</td><td>UC-118-AF01</td></tr> <tr> <td>Name</td><td>Put Patient Consent - HC Organization - Administrative working in Health Insurance Organisation</td></tr> <tr> <td>Description</td><td>An administrative working in the concerned Health Insurance Organization (HIO) under the responsibility of a doctor declares a Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS</td></tr> <tr> <td>Actor(s)</td><td> <ul style="list-style-type: none"> An administrative working in a HIO under the responsibility of a doctor </td></tr> <tr> <td>Requirements</td><td> <ul style="list-style-type: none"> End-user is an administrative working in a HIO under the responsibility of a doctor Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Identification of the admin: SSIN number, professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p> </td></tr> <tr> <td>Trigger</td><td>The user wants to declare a Patient Consent on behalf of the patient</td></tr> <tr> <td>Preconditions</td><td> <ul style="list-style-type: none"> The user has an account for the application The user is logged out </td></tr> <tr> <td>Flow</td><td> <ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using his eID A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The informed Patient Consent is stored in eHealth Database The request is logged The WS Consent responds with a Put patient consent response </td></tr> <tr> <td>Difference in flow</td><td>Identification of the end-user: Identification of the admin needs to be present</td></tr> <tr> <td>Post Condition(s)</td><td> <ul style="list-style-type: none"> Request is logged Informed Patient Consent is stored in the eHealth Database </td></tr> <tr> <td>Test Data</td><td> <ul style="list-style-type: none"> Example Request HIO Administrative Example PutPatientConsentRequest Example PutPatientConsentResponse </td></tr> </table>	ID	UC-118-AF01	Name	Put Patient Consent - HC Organization - Administrative working in Health Insurance Organisation	Description	An administrative working in the concerned Health Insurance Organization (HIO) under the responsibility of a doctor declares a Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS	Actor(s)	<ul style="list-style-type: none"> An administrative working in a HIO under the responsibility of a doctor 	Requirements	<ul style="list-style-type: none"> End-user is an administrative working in a HIO under the responsibility of a doctor Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Identification of the admin: SSIN number, professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p>	Trigger	The user wants to declare a Patient Consent on behalf of the patient	Preconditions	<ul style="list-style-type: none"> The user has an account for the application The user is logged out 	Flow	<ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using his eID A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The informed Patient Consent is stored in eHealth Database The request is logged The WS Consent responds with a Put patient consent response 	Difference in flow	Identification of the end-user: Identification of the admin needs to be present	Post Condition(s)	<ul style="list-style-type: none"> Request is logged Informed Patient Consent is stored in the eHealth Database 	Test Data	<ul style="list-style-type: none"> Example Request HIO Administrative Example PutPatientConsentRequest Example PutPatientConsentResponse
ID	UC-118-AF01																						
Name	Put Patient Consent - HC Organization - Administrative working in Health Insurance Organisation																						
Description	An administrative working in the concerned Health Insurance Organization (HIO) under the responsibility of a doctor declares a Informed Patient Consent on behalf of the patient. Using the eHealth Certificate of the HIO to access the Consent WS																						
Actor(s)	<ul style="list-style-type: none"> An administrative working in a HIO under the responsibility of a doctor 																						
Requirements	<ul style="list-style-type: none"> End-user is an administrative working in a HIO under the responsibility of a doctor Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Identification of the admin: SSIN number, professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p>																						
Trigger	The user wants to declare a Patient Consent on behalf of the patient																						
Preconditions	<ul style="list-style-type: none"> The user has an account for the application The user is logged out 																						
Flow	<ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using his eID A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The informed Patient Consent is stored in eHealth Database The request is logged The WS Consent responds with a Put patient consent response 																						
Difference in flow	Identification of the end-user: Identification of the admin needs to be present																						
Post Condition(s)	<ul style="list-style-type: none"> Request is logged Informed Patient Consent is stored in the eHealth Database 																						
Test Data	<ul style="list-style-type: none"> Example Request HIO Administrative Example PutPatientConsentRequest Example PutPatientConsentResponse 																						

	End point (s)	<ul style="list-style-type: none"> • WS Consent • eHealth Database
	Remarks	<ul style="list-style-type: none"> • If support card number is provided then it must be compliant e.g. correct format, check-digit and combination • Support card number is not mandatory if the concerned patient is a new born (0 < patient < 3 months)
	Additional Information	Additional information about the HIO, doctor, administrative e.g. software name, address, doctor name and administrative name may be added for the audit purpose

Exception Flow 1


Flow	Specifications
------	----------------



Unknown macro: 'drawio'

ID	UC-118-EF01
Name	Put Patient Consent - HC Organization - Health Insurance Organisation - Deceased patient
Description	A doctor working in the concerned Health Insurance Organization (HIO) updates an Informed Patient Consent for a deceased patient. Using the eHealth Certificate of the HIO to access the Consent WS.
Actor(s)	A doctor working in the concerned HIO
Requirements	<ul style="list-style-type: none"> • End-user is a doctor working in the concerned HIO • Valid eHealth Certificate of the HIO • Consent WS is integrated in the software of the end-user • The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software • Identification of the HIO: CBE number, HIO category • Identification of the doctor: SSIN number, NIHI (if available), the professional category • Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p> <ul style="list-style-type: none"> • Concerned patient is deceased
Trigger	The user wants to update a Patient Consent
Precondition(s)	<ul style="list-style-type: none"> • The user has an account for the application • The user is logged out
Flow	<ol style="list-style-type: none"> 1. The user attempts to access the eHealth Consent WS 2. The user needs to request a SAML Token by using the <i>eHealth Certificate of the HIO</i> 3. A request for a SAML Token is sent to the Secure Token Service (STS) 4. The STS responds with a SAML Token 5. The user has access to the eHealth WS Consent 6. The user does a request for Put Patient Consent 7. The Put Patient Consent Request is sent to the WS Consent 8. The WS Consent responds with a Put Patient Consent Response: error message
Post Condition(s)	Error message
Test Data	<ul style="list-style-type: none"> • Example PutPatientConsentRequest • Example PutPatientConsentResponse
Endpoint(s)	<ul style="list-style-type: none"> • WS Consent • eHealth Database

Exception Flow 2

Flow	Specifications																						
 Unknown macro: 'drawio'	<table border="1"> <tr> <td>ID</td><td>UC-118-EF02</td></tr> <tr> <td>Name</td><td>Put Patient Consent - HC Organization -Health Insurance Organisation - Active consent already exists for the concerned patient</td></tr> <tr> <td>Description</td><td>A doctor working in the concerned Health Insurance Organization (HIO) updates an Informed Patient Consent for a patient. Using the eHealth Certificate of the HIO to access the Consent WS. Active consent already exists for the concerned patient</td></tr> <tr> <td>Actor(s)</td><td>A doctor working in the concerned HIO</td></tr> <tr> <td>Requirements</td><td> <ul style="list-style-type: none"> End-user is a doctor working in the concerned HIO Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p> <ul style="list-style-type: none"> Active consent already exists for the concerned patient </td></tr> <tr> <td>Trigger</td><td>The user wants to put a Patient Consent</td></tr> <tr> <td>Precondition(s)</td><td> <ul style="list-style-type: none"> The user has an account for the application The user is logged out </td></tr> <tr> <td>Flow</td><td> <ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using the <i>eHealth Certificate of the HIO</i> A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The WS Consent responds with a Put Patient Consent Response: error message </td></tr> <tr> <td>Post Condition(s)</td><td>Error message</td></tr> <tr> <td>Test Data</td><td> <ul style="list-style-type: none"> Example PutPatientConsentRequest Example PutPatientConsentResponse </td></tr> <tr> <td>Endpoint(s)</td><td> <ul style="list-style-type: none"> WS Consent eHealth Database </td></tr> </table>	ID	UC-118-EF02	Name	Put Patient Consent - HC Organization - Health Insurance Organisation - Active consent already exists for the concerned patient	Description	A doctor working in the concerned Health Insurance Organization (HIO) updates an Informed Patient Consent for a patient. Using the eHealth Certificate of the HIO to access the Consent WS. Active consent already exists for the concerned patient	Actor(s)	A doctor working in the concerned HIO	Requirements	<ul style="list-style-type: none"> End-user is a doctor working in the concerned HIO Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p> <ul style="list-style-type: none"> Active consent already exists for the concerned patient 	Trigger	The user wants to put a Patient Consent	Precondition(s)	<ul style="list-style-type: none"> The user has an account for the application The user is logged out 	Flow	<ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using the <i>eHealth Certificate of the HIO</i> A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The WS Consent responds with a Put Patient Consent Response: error message 	Post Condition(s)	Error message	Test Data	<ul style="list-style-type: none"> Example PutPatientConsentRequest Example PutPatientConsentResponse 	Endpoint(s)	<ul style="list-style-type: none"> WS Consent eHealth Database
ID	UC-118-EF02																						
Name	Put Patient Consent - HC Organization - Health Insurance Organisation - Active consent already exists for the concerned patient																						
Description	A doctor working in the concerned Health Insurance Organization (HIO) updates an Informed Patient Consent for a patient. Using the eHealth Certificate of the HIO to access the Consent WS. Active consent already exists for the concerned patient																						
Actor(s)	A doctor working in the concerned HIO																						
Requirements	<ul style="list-style-type: none"> End-user is a doctor working in the concerned HIO Valid eHealth Certificate of the HIO Consent WS is integrated in the software of the end-user The consent is managed by personnel of a recognized HIO by means of their in-house applications throughout its usual software Identification of the HIO: CBE number, HIO category Identification of the doctor: SSIN number, NIHI (if available), the professional category Criteria relative to the consent <p>°Identification concerned patient: Patient SSIN, First and family name (optional)</p> <p>°Type of consent: retrospective</p> <p>°Signing date of consent</p> <ul style="list-style-type: none"> Active consent already exists for the concerned patient 																						
Trigger	The user wants to put a Patient Consent																						
Precondition(s)	<ul style="list-style-type: none"> The user has an account for the application The user is logged out 																						
Flow	<ol style="list-style-type: none"> The user attempts to access the eHealth Consent WS The user needs to request a SAML Token by using the <i>eHealth Certificate of the HIO</i> A request for a SAML Token is sent to the Secure Token Service (STS) The STS responds with a SAML Token The user has access to the eHealth WS Consent The user does a request for Put Patient Consent The Put Patient Consent Request is sent to the WS Consent The WS Consent responds with a Put Patient Consent Response: error message 																						
Post Condition(s)	Error message																						
Test Data	<ul style="list-style-type: none"> Example PutPatientConsentRequest Example PutPatientConsentResponse 																						
Endpoint(s)	<ul style="list-style-type: none"> WS Consent eHealth Database 																						