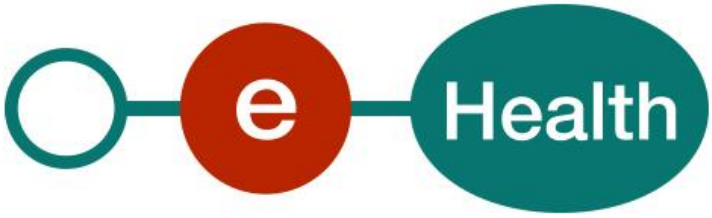


Incidents and Interventions REST service
Cookbook
Version 1.3

eHealth platform

Willebroekkaai 38 – 1000 Brussel

38, Quai de Willebroek – 1000 Bruxelles

Table of contents

To the attention of: “IT expert” willing to integrate this web service.

1. Document management

1.1 Document history

Version	Date	Author	Description of changes / remarks
1.0	17/01/2025	Smals	First version of the document by Lionell Fernandez
1.1	13/02/2025	Smals	Changes made after Mathieu's review in API Dashboard Documentation (version 1.1)
1.2	05/03/2025	Smals	Changes made after review of eHealth Service Management
1.3	19/03/2025	Smals	Changes made after review of Hannes De Clercq

2. Introduction

2.1 Goal of the service

The eHealth Incidents and Interventions REST service enables institutions to retrieve and integrate real-time information about ongoing and recently resolved incidents and interventions on the eHealth platform, facilitating transparency and enhanced coordination across healthcare systems.

2.2 Goal of the document

This document is not a development or programming guide for internal applications. Instead, it provides functional and technical information to enable an organization to integrate and use the eHealth platform service.

However, ensure smooth, consistent and risk controlled interactions with a maximum number of partners, these partners must commit to complying with the specifications, data format and release processes of the eHealth platform as described in this document.

Both technical and business requirements must be met, to allow the integration and validation of the eHealth platform service in the client application.

2.3 Service history

This chapter contains the list of changes made to the service with respect to the previous version.

Previous version	Previous release date	Changes
1.0 Current version	15/01/2025	INITIAL REST version
1.1 Second version	13/02/2025	Changes made after Mathieu De Keyzer's review in API Dashboard Documentation (version 1.1)
1.2 Third version	05/03/2025	Changes made after review of eHealth Service Management
1.3 Fourth version	19/03/2025	Changes made after review of Hannes De Clercq

3. Support

3.1 Helpdesk eHealth platform

3.1.1 Certificates

To access the secured eHealth platform environment you must obtain a eHealth platform certificate, which is used to identify the initiator of the request. If you do not have one, please consult the chapter about the eHealth certificates on the portal of the eHealth platform

- ***https://www.ehealth.fgov.be/ehealthplatform/nl/ehealth-certificaten***
- ***https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth***

For technical issues regarding eHealth platform certificates

- Acceptance: ***acceptance-certificates@ehealth.fgov.be***
- Production: ***support@ehealth.fgov.be***

3.1.2 For issues in production

eHealth platform contact centre:

- Phone: 02 788 51 55 (on working days from 7 am till 8 pm)
- Mail: ***support@ehealth.fgov.be***
- *Contact Form :*
  - ***https://www.ehealth.fgov.be/ehealthplatform/nl/contact*** (Dutch)
  - ***https://www.ehealth.fgov.be/ehealthplatform/fr/contact*** (French)

3.1.3 For issues in acceptance

Integration-support@ehealth.fgov.be

3.1.4 For business issues

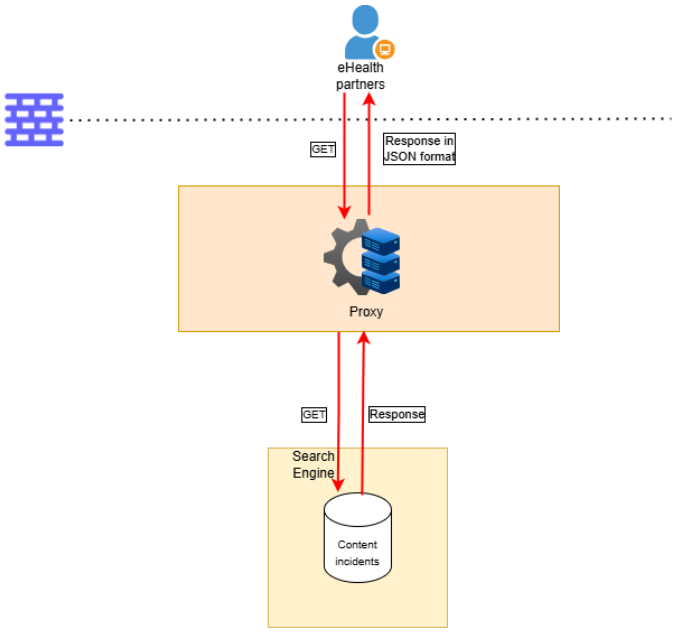
- Regarding an existing project: the project manager in charge of the application or service
- Regarding a new project or other business issues: ***info@ehealth.fgov.be***

3.2 Status

The website ***https://status.ehealth.fgov.be*** is the monitoring and information tool for the ICT functioning of the eHealth services that are partners of the Belgian eHealth system.

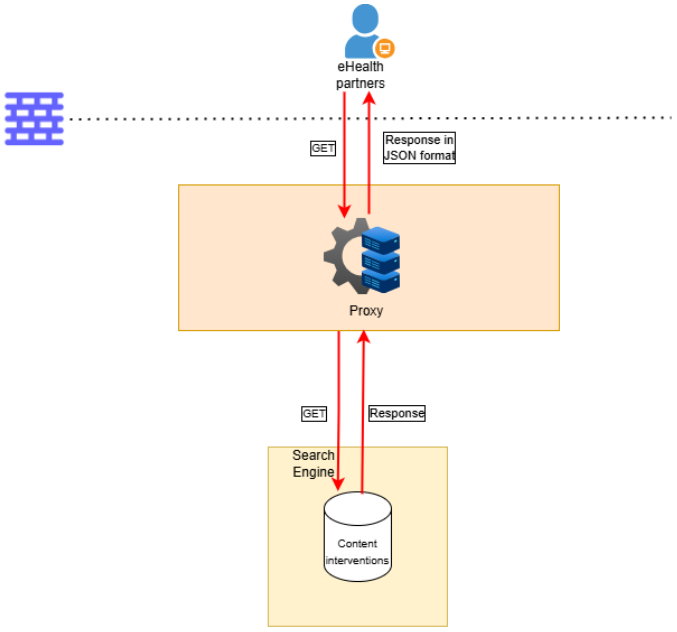
4. Global overview

Schema for incidents



URL : https://status.ehealth.fgov.be/api/v1/incidents

Schema for Interventions :



URL : https://status.ehealth.fgov.be/api/v1/interventions

5. Step-by-step

5.1 Technical requirements

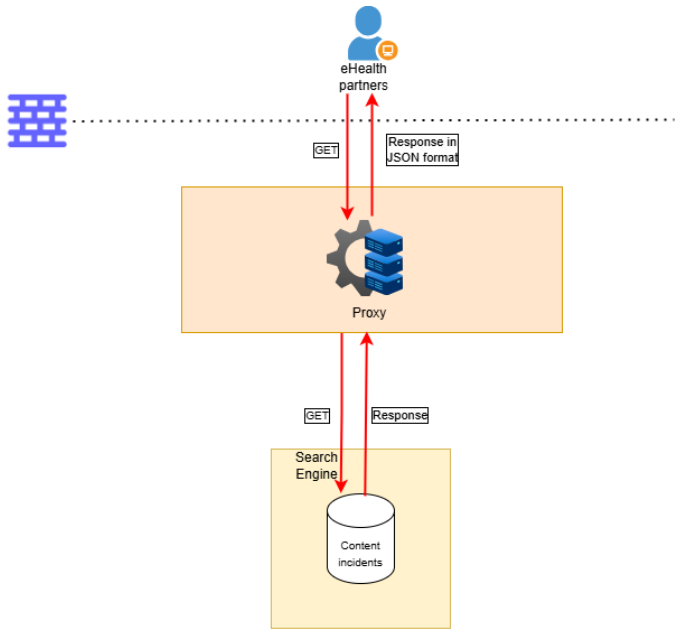
5.1.1 Tracing

To use this service, the request SHOULD contain the following two http header values (see RFC ***https://datatracker.ietf.org/doc/html/rfc7231#section-5.5.3***):

1. User-Agent: information identifying the software product and underlying technical stack/platform. It MUST include the minimal identification information of the software so that the emergency contact (see below) can uniquely identify the component.
   a. Pattern: {minimal software information}/{version} {minimal connector information}/{connector-package-version}
   b. Regular expression for each subset (separated by a space) of the pattern: [[a-zA-Z0-9-\/]*\/[0-9azA-Z-_.]*
   c. Examples:
      User-Agent: myProduct/62.310.4 Technical/3.19.0
      User-Agent: Topaz-XXXX/123.23.X freeconnector/XXXXX.XXX
2. Accept must be specified with the value application/json

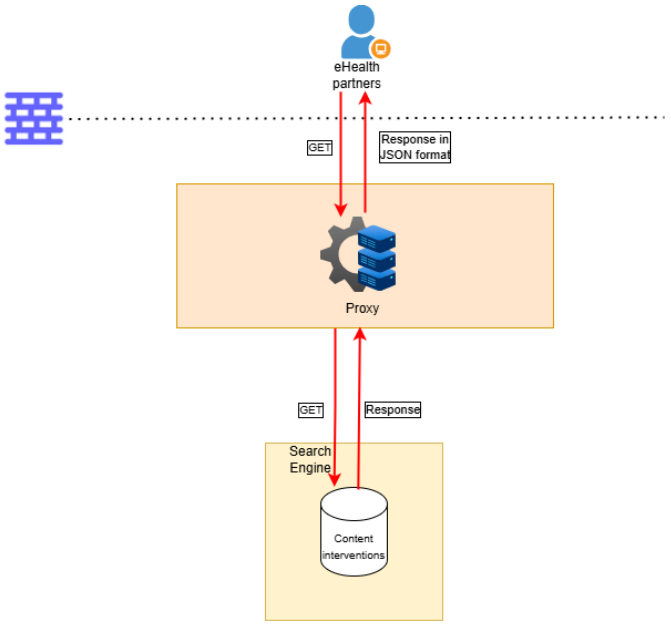
5.2 Process overview

Schema for incidents



URL : https://status.ehealth.fgov.be/api/v1/incidents

Schema for Interventions :



URL : https://status.ehealth.fgov.be/api/v1/interventions

The eHealth partners send a GET request to retrieve data of an incident or intervention via an URL :

- Incidents :
  - https://status.ehealth.fgov.be/api/v1/incidents
- Interventions
  - https://status.ehealth.fgov.be/api/v1/interventions

The response is in JSON format.

5.3 Web service

5.3.1 Method #1

5.3.1.1 Input arguments #1

The eHealth partner sends a GET request via an URL : https://status.ehealth.fgov.be/api/v1/interventions

5.3.1.2 Output arguments #1

The response is in JSON format.

Below is an example of JSON Response for an intervention :


```
{
  "data": [
    {
      "identifier": "1447",
      "name": "Firewall switch-over",
      "start_datetime": "2025-02-16T22:00:00+0100",
```

```
      "end_datetime": "2025-02-16T22:15:00+0100",
      "closed": false,
      "description": "<p>The firewall cluster will be switched over to another dat
a center.</p>\r\n\r\n<div class=\"WordSection1\">\r\n<p style=\"margin-top:2.0pt;
margin-right:0cm; margin-bottom:2.0pt; margin-left:0cm\"> </p>\r\n</div>",
      "business_impact": "without_business_impact",
      "intervention_type": "emergency",
      "impact": "<p>The connection may be interrupted for a few minutes. Othe
r than that, the intervention will likely have no impact on the availability
of the eHealth services. </p>",
      "provider": "Smals",
      "type": "intervention"
    }
  ]
}
```


Field name	Description
identifier	A unique ID or reference number for the intervention.
name	The name of the intervention (e.g., "Firewall switch-over")
start_datetime	The start date and time of the event in ISO 8601 format (e.g., "2025-02-16T22:00:00+0100")
end_datetime	The end date and time of the event in ISO 8601 format (e.g., "2025-02-16T22:15:00+0100")
closed	A Boolean (checkbox field type) indicating whether the event is closed: false (unchecked) → The intervention is still open. true (checked) → The intervention has been closed (it is done).
description	A free-text field where the user provides a description of the scope of the intervention. In the JSON response, the description is stored with HTML formatting (e.g., " The firewall cluster will be switched over to another data center. ").
business_impact	A radio button field indicating the business impact. It has two possible values: **with_business_impact** or **without_business_impact**.
type_intervention	A radio button field for selecting the type of intervention. Possible values: **standard** or **emergency**.
impact	A free-text field where the user provides a description of the impact of the event. In the JSON response, it is stored with HTML formatting (e.g., " The connection may be interrupted for a few minutes. Other than that, the intervention will likely have no impact on the availability of the eHealth services. ").
provider	The name of the service provider responsible for the intervention. The user must select one valid institution from a dropdown list containing 27 predefined options (e.g., "Smals").

type	The general classification of the record.

5.3.2 Method #2

5.3.2.1 Input arguments #2

The eHealth partner sends a GET request via an URL : https://status.ehealth.fgov.be/api/v1/incidents

5.3.2.2 Output arguments #2

Below an example of a JSON response for an incident :


```
{
  "data": [
    {
      "identifier": "43537",
      "name": "IO 900 incident test",
      "start_datetime": "2025-03-11T10:20:00+01:00",
      "end_datetime": "2025-03-11T11:20:00+01:00",
      "status": "Solved",
      "impact": "<p>Impact low</p>",
      "description": "<p>Due to an unplanned patching, our production platform enc
ountered small perturbation.</p>",
      "contact_info": "<p>900-carenet-mycarenet@hr-rail.be</p>",
      "update": false,
      "provider": "CIN-NIC",
      "type": "incident"
    }
  ]
}
```


Field name	Description
identifier	A unique identifier for this specific incident (e.g., "43537").
title	The title of the incident (e.g., "IO 900 incident test")
start_datetime	The start date and time of the incident in ISO 8601 format (e.g., "2025-03-11T10:20:00+01:00").
end_datetime	The end date and time of the incident in ISO 8601 format (e.g., "2025-03-11T11:20:00+01:00").
status	The current status of the incident :

	By default, if no end_datetime is defined, the status is “Ongoing”. If an end_datetime is defined, the status changes to “Solved”.
impact	A free-text field where the user describes the impact of the incident. In the JSON response, the content is automatically converted into HTML (e.g., " Impact low ").
description	A free-text field where the user provides details about the incident. In the JSON response, the description is automatically converted into HTML (e.g., " Due to an unplanned patching, our production platform encountered small perturbation. ”)
contact_info	A free-text field where the user provides contact information for further inquiries. In the JSON response, the content is automatically converted into HTML (e.g., "smals@info.be").
update	A boolean (checkbox field type) indicating whether there is an update available. False (unchecked) → There is no update True (checked) → There is an update
provider	The name of the service provider involved in the incident. The user must select one valid institution from a dropdown list containing 27 predefined options (e.g., "CIN-NIC").
type	The general classification of the record.

6. Risks and security

6.1 Security

6.1.1 Business security

If the development adds a use case based on an existing integration, the eHealth platform must be informed at least one month in advance. A detailed estimate of the expected load is necessary to be able to ensure effective capacity management.

When technical issues occur with the WS, the partner can obtain support from the contact centre (see Chap 3)

If the eHealth platform identifies a bug or vulnerability in its software, the partner must update his application with the latest version of the software, within ten (10) business days.

If the partner finds a bug or vulnerability in the software or web service provided by the eHealth platform, he is obliged to contact and inform us immediately. He is not allowed, under any circumstances, to publish this bug or vulnerability.

6.1.2 Web service

WS security used in this manner is in accordance with the common standards. Your call will provide:

6.1.3 SSL one wayThe use of username, password and token

Not applicable

7. Test and release procedure

7.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptation or production.

7.1.1 Initiation

If you intend to use the eHealth platform service, please contact:
ehealth_service_management@ehealth.fgov.be

The project department will provide you with the necessary information and mandatory documents.

7.1.2 Development and test procedure

You need to develop a client to connect to our WS. Most of the information for integration is published on the portal of the eHealth platform.

Upon request and depending on the case, the eHealth platform provides you with a **test case** to test your client before releasing it in the acceptance environment.

7.1.3 Release procedure

When development tests are successful, you can request access to the acceptance environment of the eHealth platform. From this moment, you begin the integration and acceptance tests. The eHealth platform suggests testing for a minimum of one month.

After successful acceptance tests, the partner sends his test and performance results, along with a sample of "eHealth request" and "eHealth answer" by email to his point of contact at the eHealth platform.

Once a release date has been agreed upon, the eHealth platform prepares the connection to the production environment and provides the partner with the necessary information. On the release day, the partner provides the eHealth platform with feedback on the test and performance results.

For further information and instructions, please contact: ***integration-support@ehealth.fgov.be***.

7.1.4 Operational follow-up

Once in production, the partner using the eHealth platform service for one of his applications must always test in the acceptance environment first before releasing any adaptations of his application in production. In addition, he will inform the eHealth platform on the progress and test period.

7.2 Test cases

The eHealth platform recommends performing tests for all of the following cases:

- https://status-sim.ehealthplatform.info/api/v1/interventions
- https://status-sim.ehealthplatform.info/api/v1/incidents

8. Error and failure messages

We rely on standard HTTP error codes