FHIR Client Development Guide

November 17, 2022

Table of Contents

[Introduction 1](#_Toc119658294)

[Integration with EDRS System 1](#_Toc119658295)

[Authentication 2](#_Toc119658296)

[Configurable parameters 2](#_Toc119658297)

[Timeliness 2](#_Toc119658298)

[Configurable parameters 2](#_Toc119658299)

[Message Resends 2](#_Toc119658300)

[Configurable parameters 3](#_Toc119658301)

[Response Message Handling 3](#_Toc119658302)

[Configurable parameters 3](#_Toc119658303)

[Message Traceability 3](#_Toc119658304)

[NCHS Backup Endpoint 4](#_Toc119658305)

[Configurable parameters: 4](#_Toc119658306)

# Introduction

The NVSS FHIR Modernization effort will implement the exchange of FHIR messages between jurisdiction’s and NCHS for mortality data. NCHS has implemented a test FHIR API server for jurisdictions to submit their mortality data. Each jurisdiction will implement a client that exchanges FHIR data with the NCHS server. A jurisdiction’s client implementation must follow the messaging protocol described in the [FHIR Messaging IG](http://build.fhir.org/ig/nightingaleproject/vital_records_fhir_messaging_ig/branches/main/message.html) to ensure reliable message delivery and traceability. The [Reference Client](https://github.com/nightingaleproject/Reference-Client-API) is an open-source example of a C# implementation of the FHIR Messaging IG. Implementers may leverage the Reference Client, tools such as Rhapsody, or develop a custom solution to communicate with the API. In general, each Client implementation should support the following guidelines when deployed to production. Each section species configurable parameters that should be defined in a separate config file.

# Integration with EDRS System

The client must be integrated with the jurisdiction’s EDRS system so that FHIR Death Records produced by the EDRS system are submitted to the FHIR API by the client.

The client should be capable of submitting the following message types to the API:

* Submission Message
* Update Message
* Alias Message
* Void Message
* Acknowledgements

# Authentication

The client must support authentication to the FHIR API gateway

* + Jurisdictions must have STEVE credentials. STEVE credentials must be used by the client to make authenticated requests to STEVE to submit data to the FHIR API on behalf of the jurisdiction
  + Jurisdictions must have SAMS credentials. SAMS credentials must be used by the client to make authenticated requests to the backup API endpoint

The client should support automatic authentication refresh

* + The STEVE auth token expires after 5 minutes. Client systems should be capable of auto refreshing their token for uninterrupted communications.
  + The SAMS auth token expires after 1 hour. Client systems should be capable of auto refreshing their token for uninterrupted communications.

## Configurable parameters

* STEVE Username
* STEVE Password
* STEVE Client Secret
* STEVE Client Token
* STEVE Authentication endpoint
* SAMS Username
* SAMS Password
* SAMS Client Secret
* SAMS Client Token
* SAMS Authentication endpoint

# Timeliness

The client must submit FHIR messages in a timely manner. It is recommended that once a Death Record is entered into the EDRS system, it be submitted as soon as it becomes available, ideally within 1 hour.

The client must support polling the FHIR API to regularly check for FHIR message responses from NCHS. It is recommended to poll the FHIR API at least once every 5 minutes.

## Configurable parameters

* Submission interval
* Polling interval

# Message Resends

The client must support resends if a message is not acknowledged within the configured time frame. The resubmission message header must be identical to the initial submission message header. The header date timestamp must be identical to the initial message to preserve the order the submission message and any update messages should be processed by NCHS. It is recommended to save the json bundle to preserve the exact message in case there is a need to resubmit. The current recommended resend window is 5 hours.

The maximum number of retries should be 3. After 3 attempts and no acknowledgements, a jurisdictional contact at NCHS should be notified via email or some other notification system. Jurisdictions should identify someone on their end of the system who is responsible for monitoring failed messages who will receive and respond to these notifications.

The current recommendation is to implement an “exponential” back off when resending messages.

1. 5 hours
2. 10 hours
3. 20 hours

## Configurable parameters

* Resend interval
* Maximum retries

# Response Message Handling

The client must handle the following message response types

* + Acknowledgements (ACK)
  + Extraction Errors (ERR)
  + Cause of Death Coding Responses (TRX)
  + Demographic Coding Responses (MRE)
  + Status Response (STM)

The client must acknowledge the following message response types

* + Cause of Death Coding Responses (TRX)
  + Demographic Coding Responses (MRE)

The client should support acknowledging response messages in a timely manner to avoid unnecessary duplicate messages from NCHS. Acknowledgements should be sent as soon as they become available and no more than 3 hours after.

## Configurable parameters

* Submission interval

# Message Traceability

The client must maintain a persistent store of Death Records submitted to NCHS. It is recommended to make the message ID of past records easily accessible for traceability.

The client must support tracing message responses to their initial submission so they can track the status of that message. Use the message ID of the submitted message and the reference message ID in message responses to implement traceability.

The client should provide an easy method to see the status of submitted messages and identify records that resulted in an Extraction Error and require modification.

# NCHS Backup Endpoint

The client must be configured to submit messages to STEVE by default and to NCHS as a backup when STEVE is unavailable. Jurisdictions should only submit messages to the backup endpoint when NCHS directs them to switch from STEVE to the back up endpoint.

## Configurable parameters:

* STEVE endpoint
* NCHS backup endpoint