Novitas Solutions, Inc.
Hypertext Transfer Protocol Secure (HTTPS) Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules (CORE)-Compliant Connection for Electronic Data Interchange (EDI) Connectivity Guide

Contents

Introduction

This document provides information on the HTTPS CAQH CORE-Compliant Connection for EDI: how to connect to the Novitas TIBCO system server, message envelope standards and message exchanges, Hypertext Transfer Protocol & Multipurpose Internet Mail Extensions (HTTP+MIME), and Simple Object Access Protocol & Web Service Definition Language (SOAP+WSDL) Message over the public internet in accordance with the CAQH CORE Phase II Connectivity Rule 270.

HTTPS CAQH CORE Supported Transactions:

The following EDI transactions are supported in batch mode.

1. Health Care Claim Status Request and Response (276/277)
2. Health care Claim Payment Advice (835)
3. Implementation Acknowledgement for Health Care Insurance (999)

More information on CAQH CORE Connectivity Rule 270 version 2.2.0 is available at:
https://www.caqh.org/sites/default/files/core/phase-ii/Phase%20II.Connectivity%20Rule.pdf

User Expectations

This document is intended for use by a technical professional or organization that has experience implementing secure web-based connectivity. The instructions in this guide are not intended to stand alone as a sole resource.

It is solely the responsibility of the submitter or user to develop and create their CORE Web Services-compliant client application. Novitas will not provide or support the end user client application. We strongly recommended that the organization using this guide take appropriate action to have available technical support before attempting to enroll for use of this connectivity method.

Please ensure you are using Soap Envelope Version 1.2 and SOAP Message Version 1.2. Also make sure you are using Transport Security Mode with Certificate Authentication.

Enrollment

Users must enroll with Novitas EDI Services for the HTTPS CAQH CORE-compliant connection for EDI.

To enroll, users must complete the appropriate HTTPS CAQH CORE Enrollment form.

- **JL Forms:**
  - http://www.novitas-solutions.com/webcenter/portal/MedicareJL/pagebyid?contentId=00147500
- **JH Forms:**
  - http://www.novitas-solutions.com/webcenter/portal/MedicareJH/pagebyid?contentId=00147500

X.509 Digital Certificate Requirements

Trading partners will need to authenticate with an X.509 digital certificate. User ID and password authentication will not be supported. Trading partners will need to obtain an X.509 digital certificate from a trusted certificate authority. The trading partner's X.509 digital certificate must be submitted to the Novitas EDI gateway TIBCO server via Secure File Transfer Protocol (SFTP). Please refer to the list of approved Network service vendors:

- **JL:** https://www.novitas-solutions.com/webcenter/portal/MedicareJL/pagebyid?contentId=00004536
- **JH:** https://www.novitas-solutions.com/webcenter/portal/MedicareJH/pagebyid?contentId=00004536

To submit the X.509 Digital Certificate:

- Save the certificate with a valid filename extension. The valid filename extensions allowed are:
  - *.cer
  - *.crt
  - *.der
  - *.pem

- Connect via SFTP. Refer to your NSV for more information.
- Submit the X.509 certificate to folder, */outbox/EZComm/BC/1.0/Notify*
- Once the X.509 certificate has been submitted via SFTP, please contact Novitas EDI Services to complete the loading of the X.509 certificate to your EDI profile to support authentication.

Once you have submitted a successful X.509 certificate, and EDI Services has loaded the X.509 certificate to your profile, you may proceed with connecting and submitting your files.

Connectivity URLs

EDI Submitters connecting via SOAP will use the following link to connect, send, and receive their EDI transactions.

- https://edi-uat.guidewellsource.com:16707/SOAP?host={Tibco BC HOST Entity}&tpname={SubmitterId}&opid=CAQH/2.2.0/BatchSubmitTransaction&transid={Payload ID}
    - Example: https://edi-uat.guidewellsource.com:16707/SOAP?host=GuideWell Source&tpname=SubmitterId&opid=CAQH/2.2.0/BatchSubmitTransaction&transid=20201211-2320-4a0e-9ef7-154911341570

Please Note: The addition of the Host, Submitter ID and Payload ID fields to the above URLs, are likely to cause interoperability problems for trading partners that deal with multiple entities unless trading partners agree on their syntax and semantics of each entity prior to installation.

Envelope Data Element Definitions

CAQH CORE connectivity rule 270 defines the envelope requirements and envelope metadata. These are payer specific requirements for SOAP and MIME.

Element	Value
Sender ID	Novitas EDI assigned Submitter ID as provided on your EDI Welcome Letter.
Receiver ID	This should be the receiver ID ISA08/GS03 from the X12 payload file.
Payload ID	Unique identifier for a transaction submission. Must be unique for each transaction.
Payload Type	Reference the different EDI transaction examples in the CAQH CORE Connectivity Rule 270.

A Payload ID must be included in the request to download a “RECEIVE.999” or a “RECEIVE.TA1”, to identify the specific Ack to Retrieve. This ties the 999 and the TA1 back to the 276 they were generated from.

A Payload ID is not used to download a “RECEIVE.277_5010” or a “RECEIVE.835_5010”. If there are multiple 277 or 835 files available when the CAQH request is submitted, all available files will be concatenated and sent at the same time.

Client Software Requirements

Users will need client software that is compliant with the CORE Standards outlined on the CAQH-CORE website to utilize the HTTPS CAQH CORE-Compliant Connection. A link to the CAQH CORE 270 Connectivity rule is provided in the reference material below. Please reference this information to develop the user's client software.

Novitas cannot assist the user in developing this client software, nor does Novitas have sample software available. Novitas also does not support the user's client software.

References

- CORE Connectivity Rule 270 for SOAP and MIME: https://www.caqh.org/sites/default/files/core/phase-ii/Phase%20II.Connectivity%20Rule.pdf
- WSDL Information: https://coregateway.novitas-solutions.com/CoreBatchGateway/soap/coreservice?wsdl

SOAP and MIME Common Error Handling:

Use expired Cert via SOAP:
BatchSubmitTransaction exception: Could not establish secure channel for SSL/TLS with authority
Use expired Cert via MIME:
The request was aborted: Could not create SSL/TLS secure channel.

Use revoked Cert via SOAP:
Valid certificate not found.
Use revoked Cert via MIME:
InternalError An unexpected error has occurred while processing the transaction.

Use future Cert via SOAP:
Could not establish secure channel for SSL/TLS with authority
Use future Cert via MIME:
The request was aborted: Could not create SSL/TLS secure channel.

Use deleted Cert via SOAP
Valid certificate not found.
Use deleted Cert via MIME
InternalError An unexpected error has occurred while processing the transaction.

SOAP test with suspended user:
UnAuthorized The username/password or Client certificate could not be verified.
MIME test with suspended user:
UnAuthorized The username/password or Client certificate could not be verified.