

NE Medicaid

Department of Health & Human Services



DIVISION OF MEDICAID AND LONG-TERM CARE

Publication Date: 05/19/2015

Effective Date: 05/19/2015

Submission and Connectivity Guide using HTTP/S

Version 3.1

DHHS.MedicaidEDI@Nebraska.gov

EDI Help Desk (866) 498-4357

Preface

Nebraska Medicaid is supporting Hyper Text Transfer Protocol Secure (HTTP/S) in accordance with this guide.

This Submission and Connectivity Guide for real-time and batch 270/271 and 276/277 follows the CAQH CORE Phase I and Phase II guidelines along with the batch 835 for CAQH CORE Phase III guidelines. This Submission and Connectivity Guide is prepared for use by Trading Partners affiliated with Nebraska Medicaid. This Submission and Connectivity Guide is considered a living document, and as such, the information provided herein will be subject to change.

To read a copy of the document, including any changes, will be posted via the NE Medicaid website located at:

<http://dhhs.ne.gov/medicaid/Pages/edireq-5010.aspx>

This Submission and Connectivity Guide to the Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for the Information Exchange (CORE) Operating rules 153, 270 (Safe Harbor Connectivity) and 350 (Healthcare Claim Payment/ Advice) adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) clarifies and specifies the data content when exchanging transactions electronically with Nebraska Medicaid.

This Submission and Connectivity Guide is intended to convey information that is within the framework of the CAQH CORE Operating Rules 153, 270 & 350 adapted for use under HIPAA. The guide is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the CAQH CORE Operating Rules 153, 270 & 350.

Two Trading Partner environments exist – one for test and one for production. The Trading Partner number for both environments will be the same. It is up to the Trading Partner to send the correct value in the ISA15 element and this must correspond with the environment they are submitting to.

The servers are available 24 hours a day, 7 days a week. The servers are supported by the DHHS EDI Helpdesk staff between the hours of 8:00 A.M. and 5:00 P.M. CT Monday through Friday, except State and Federal holidays. Visit the following State of Nebraska Web site to view a listing of all Nebraska state holidays: http://dhhs.ne.gov/Pages/hur_holidays.aspx.

The contact for setting up a Trading Partner ID for electronic transactions is the EDI Help Desk at (866) 498-4357. All Trading Partner IDs will start with "XEC" and will be followed by a four-digit Trading Partner number, an environment letter and the Processing Mode.

Examples are:

XEC0018TB - Test batch mode

XEC0018PB - Production batch mode

XEC0018TRT - Test real time mode

XEC0018PRT - Production real time mode.

Contents

1. CONNECTIVITY WITH THE PAYER/COMMUNICATIONS	5
1.1 PROCESS FLOW FOR REAL-TIME	5
1.2 PROCESS FLOW FOR BATCH.....	6
2. TRANSMISSION/RE-TRANSMISSION ADMINISTRATIVE PROCEDURES.....	7
3. COMMUNICATION PROTOCOL SPECIFICATIONS	7
3.1 SOAP: REAL-TIME*	9
3.2 MIME MULTIPART: REAL-TIME*	9
3.3 SOAP: BATCH.....	12
3.4 MIME: BATCH.....	13
3.5 HTTP RESPONSES/ERROR MESSAGES.....	16
3.6 ENVELOPE RESPONSES/ERROR MESSAGES.....	16
3.7 BATCH RESPONSE AND RETRIEVAL	17
4. PASSWORDS.....	17

Revision History

Date	Version	Description	Author
10-22-2014	3.0	Initial Draft for Review	Irene May
05-04-2015	3.1	Added Information related to 835 Transaction	Sagar Sankepally

Reviewers

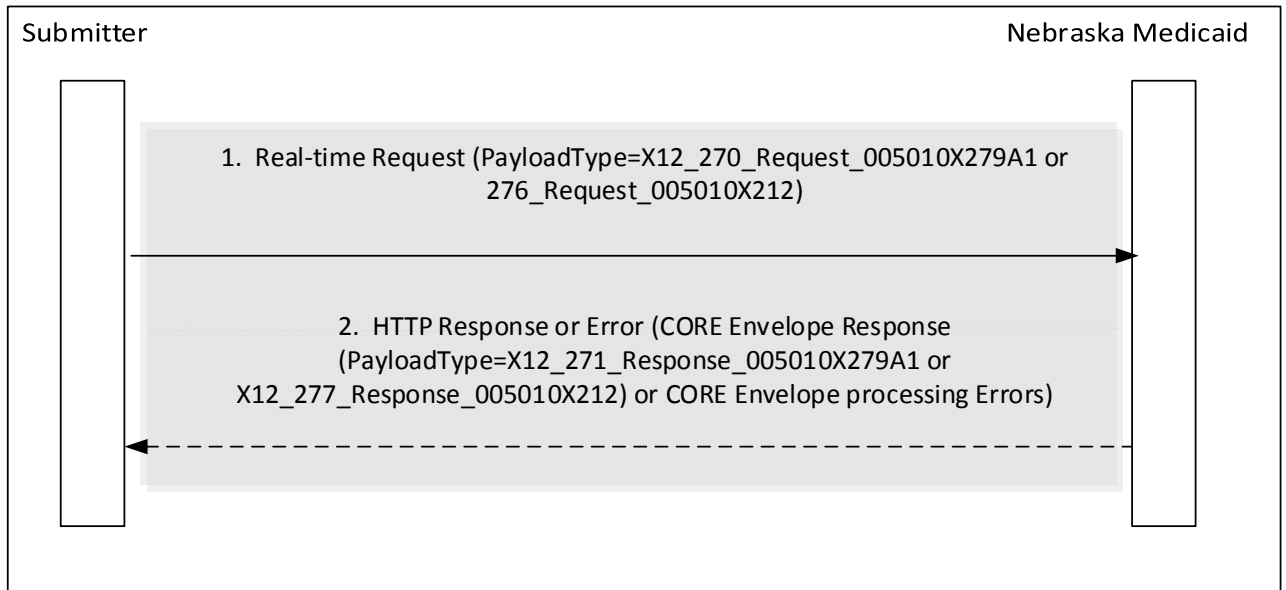
Date	Version	Description	Author

Approvers

Date	Version	Description	Author

1. CONNECTIVITY WITH THE PAYER/COMMUNICATIONS

1.1 PROCESS FLOW FOR REAL-TIME



1.2 PROCESS FLOW FOR BATCH



2. TRANSMISSION/RE-TRANSMISSION ADMINISTRATIVE PROCEDURES

Real-Time and Batch 270/271 and 276/277 transactions through HTTP/S: Real-time requests are limited to one inquiry per transaction. Batch 270 requests are limited to 99 patient requests within an ST/SE grouping. A response to the batch inquiry will be provided by 7 a.m. CT the following business day for batches received before 9 p.m. CT the previous day. Batch requests submitted after 9 p.m. CT will be available by 7 a.m. CT two business days following submission.

Batch 835 transactions through HTTP/S: All retrieval requests received from the Trading Partner through HTTP/S will be processed by NE Medicaid, provided the Trading Partners choose to receive the v5010 X12 835 Transaction. Acknowledgements sent by the Trading Partners will be accepted by NE Medicaid.

The following links below provide more information on:

System Maintenance:

Please refer to the respective Nebraska Medicaid page for the most up-to-date information on the system availability at:

<http://dhhs.ne.gov/medicaid/Pages/HTTPS-Connectivity-and-Downtime-Information.aspx>

System Downtime:

All scheduled downtimes will be published in the below link:

<http://dhhs.ne.gov/medicaid/Pages/HTTPS-Connectivity-and-Downtime-Information.aspx>

For emergency downtimes, Trading Partners will be notified via a Trading Partner Alert/email within an hour of realizing downtime is needed.

3. COMMUNICATION PROTOCOL SPECIFICATIONS

In compliance with Core rules, Nebraska Medicaid requires that all SOAP transactions conform to SOAP Version 1.2. The following files must be saved to the workstation in the same location in order to submit requests through SOAP UI.

The XML schema definition set forth by CORE and used by Nebraska Medicaid EDI is located at:

<http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd>

The WDSL definition set forth by CORE and used by Nebraska Medicaid EDI is located at:

<http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.wsdl>

The following information should be used for Trading Partner testing:

NEBRASKA MEDICAID	MODE	TRANSACTION	Request Submission to URL
SOAP + WSDL	Secure Web Service	Real-time X12 270/271 and 276/277	https://COREWEBTEST-DHHS.NE.GOV:10800/soap
	Secure Web Service	Batch X12 270/271 and 276/277	https://COREWEBTEST-DHHS.NE.GOV:10900/soap
	Secure Web Service	Batch X12 835	https://COREWEBTEST-DHHS.NE.GOV:10700/soap
HTTP + MIME	Secure Web Service	Real-time X12 270/271 and 276/277	https://COREWEBTEST-DHHS.NE.GOV:10800/multipart
	Secure Web Service	Batch X12 270/271 and 276/277	https://COREWEBTEST-DHHS.NE.GOV:10900/multipart
	Secure Web Service	Batch X12 835	https://COREWEBTEST-DHHS.NE.GOV:10700/multipart

The following information should be used for Trading Partner production:

NEBRASKA MEDICAID	MODE	TRANSACTION	Request Submission to URL
SOAP + WSDL	Secure Web Service	Real-time X12 270/271 and 276/277	https://COREWEB-DHHS.NE.GOV:10800/soap
	Secure Web Service	Batch X12 270/271 and 276/277	https://COREWEB-DHHS.NE.GOV:10900/soap
	Secure Web Service	Batch X12 835	https://COREWEB-DHHS.NE.GOV:10700/soap
HTTP + MIME	Secure Web Service	Real-time X12 270/271 and 276/277	https://COREWEB-DHHS.NE.GOV:10800/multipart
	Secure Web Service	Batch X12 270/271 and 276/277	https://COREWEB-DHHS.NE.GOV:10900/multipart
	Secure Web Service	Batch X12 835	https://COREWEB-DHHS.NE.GOV:10700/multipart

3.1 SOAP: REAL-TIME*

Message Content Details:

Payload Type: Payload Type specifies the type of payload included within a request.

Valid values are:

Request

X12_270_Request_005010X279A1

X12_276_Request_005010X212

Response

X12_271_Response_005010X279A1

X12_277_Response_005010X212

X12_999_Response_005010X231A1

X12_TA1_Response_00501X231

CoreEnvelopeError

Processing Mode: Processing Mode indicates Real-time processing mode.

Valid value is **RealTime**

Payload ID: This Identifier is used to uniquely identify the request submitted. Values are Alphanumeric, may contain hyphen.

Timestamp: Time and Date specifying when a message is created and sent to a receiver. Valid value follows standard Universal Time (UTC)

<http://www.w3.org/TR/xmlschema11-2/#dateTime>

Sender ID: Submitter ID/Client ID Valid value is alphanumeric between 4 and 15 characters as specified by the Trading Partner on the Trading Partner Profile form.

Receiver ID: NEBRASKA MEDICAID's ID valid value is alphanumeric as specified on the Trading Partner Profile form. i.e. **MMISNEBR**

CORE Rule Version: The CORE Rule version 2.2.0 is used for this envelope.

Payload: Payload contains compliant X12 270 request data or X12 276 request data. Payload should be encrypted using BASE 64 encode.

3.2 MIME MULTIPART: REAL-TIME*

HTTP Headers: For MIME multipart the messages should always contain Content-Type that specifies the boundary used to separate each part of the message.

Example:

Content-Type: multipart/form-data; boundary=XbCY

* **Note:** 835 Transaction is not applicable for Real-Time through SOAP/MIME.

Message Content Details:

Payload Type: Payload Type specifies the type of payload included within a request.

Valid values are:

Request

X12_270_Request_005010X279A1
X12_276_Request_005010X212

Response

X12_271_Response_005010X279A1
X12_277_Response_005010X212
X12_999_Response_005010X231A1
X12_TA1_Response_00501X231
CoreEnvelopeError

Processing Mode: Processing Mode indicates real-time processing mode.

Valid value is **RealTime**

Payload ID: This is an Identifier used to uniquely identify the request submitted. Values are Alphanumeric, may contain hyphen.

Time Stamp: Time and Date specifying when a message is created and sent to a receiver. Valid value follows standard Universal Time (UTC)

<http://www.w3.org/TR/xmlschema11-2/#dateTime>

Sender ID: Submitter ID/Client ID. Valid value is alphanumeric as specified by the Trading Partner on the Trading Partner Profile form.

Receiver ID: NEBRAKSA MEDICAID's ID Valid value is alphanumeric as specified on the Trading Partner Profile form. i.e. **MMISNEBR**

CORE Rule Version: The CORE Rule version 2.2.0 is used for this envelope.

Payload: Payload contains compliant X12 270 request data or X12 276 request data. Payload should be encrypted using BASE 64 encode.

Example:

```
--XbCY
Content-Disposition: form-data; name="PayloadType"
X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"
RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"
e51d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"
2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"
YOURIDHERE
--XbCY
Content-Disposition: form-data; name="ReceiverID"
MMISNEBR
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"
2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"
ISA*00* *00* *ZZ...
--XbCY—
```

3.3 SOAP: BATCH

HTTP Headers: For MTOM the messages should always contain Content-Type that specifies among others the boundary used to separate each part of the message.

Please refer to the below link for CORE Phase II Rule 270 Connectivity Rule v. 2.2.0

for examples pertaining to HTTP Headers.

<http://www.caqh.org/pdf/CLEAN5010/PIIv5010Complete.pdf>

Message Content Details:

Payload Type: Payload Type specifies the type of payload included within a request.

Valid values are:

Request

X12_270_Request_005010X279A1
X12_276_Request_005010X212

Response from Request

X12_BatchReceiptConfirmation
CoreEnvelopeError

Results Retrieval Request

X12_005010_Request_Batch_Results_271
X12_005010_Request_Batch_Results_277
X12_TA1_RetrievalRequest_00501X231A1
X12_999_RetrievalRequest_005010X231A1

Response from Results Retrieval Request

X12_271_Response_005010X279A1
X12_277_Response_005010X212
X12_999_Response_005010X231A1
X12_TA1_Response_00501X231A1
CoreEnvelopeError

Retrieval Request

X12_835_Request_005010X221A1

Response from Retrieval Request

X12_835_Response_005010X221A1
X12_005010_Response_NoBatchResultsFile
CoreEnvelopeError

Acknowledgement Submission

X12_TA1_SubmissionRequest_00501X231A1
X12_999_SubmissionRequest_005010X231A1

Response from Acknowledgement Submission

X12_Response_ConfirmReceiptRecieved
CoreEnvelopeError

Processing Mode: Processing Mode indicates Batch.

Valid value is **Batch**

Payload ID: This is an Identifier that will be used to uniquely identify the request submitted. Values are Alphanumeric, may contain hyphen. (No unique Payload ID is needed for 835 retrieval request and response).

Payload Length: Defines the length of the actual X12 payload in bytes.

Timestamp: Time and Date specifying when a message is created and sent to a receiver. Valid value follows standard Universal Time (UTC).

<http://www.w3.org/TR/xmlschema11-2/#dateTime>

Sender ID: Submitter ID/Client ID. Valid value is alphanumeric between 4 and 15 characters as specified by the Trading Partner on the Trading Partner Profile form.

Receiver ID: NEBRASKA MEDICAID'S ID Valid value is alphanumeric as specified on the Trading Partner Profile form. i.e. **MMISNEBR**

CORE Rule Version: The CORE Rule version 2.2.0 is used for this envelope.

Checksum: An element used to allow receiving site to verify the integrity of the message that is sent. Algorithm is SHA-1, encoding is Hex. Checksum must be computed only on the payload and not on the metadata (not applicable for retrieval request).

Payload: Payload contains compliant X12 270 request data or X12 276 request data. Payload should be encrypted using BASE 64 encode (not applicable for retrieval request).

3.4 MIME: BATCH**MIME Multipart: Batch**

HTTP Headers: For MIME multipart the messages should always contain Content-Type that specifies the boundary used to separate each part of the message.

Example:

Content-Type=multipart/form-data; boundary=XbCY

Message Content Details:

Payload Type: Payload Type specifies the type of payload included within a request.

Valid values are:

Request

X12_270_Request_005010X279A1

X12_276_Request_005010X212

Response from Request

X12_BatchReceiptConfirmation

CoreEnvelopeError

Results Retrieval Request

X12_005010_Request_Batch_Results_271

X12_005010_Request_Batch_Results_277

X12_TA1_RetrievalRequest_00501X231A1

X12_999_RetrievalRequest_005010X231A1

Response from Results Retrieval Request

X12_271_Response_005010X279A1

X12_277_Response_005010X212

X12_999_Response_005010X231A1

X12_TA1_Response_00501X231A1

CoreEnvelopeError

Retrieval Request

X12_835_Request_005010X221A1

Response from Retrieval Request

X12_835_Response_005010X221A1

X12_005010_Response_NoBatchResultsFile

CoreEnvelopeError

Acknowledgement Submission

X12_TA1_SubmissionRequest_00501X231A1

X12_999_SubmissionRequest_005010X231A1

Response from Acknowledgement Submission

X12_Response_ConfirmRecieptRecieved

CoreEnvelopeError

Processing Mode: Processing Mode indicates Batch.

Valid value is **Batch**

Payload ID: This is an Identifier that you will use to uniquely identify the request submitted (No unique Payload ID is needed for 835 retrieval request and response). Values are Alphanumeric, may contain hyphen.

Payload Length: Defines the length of the actual payload in bytes.

Timestamp: Time and Date specifying when a message is created and sent to a receiver. Valid value follows standard Universal Time (UTC).

<http://www.w3.org/TR/xmlschema11-2/#dateTime>

Sender ID: Submitter ID/Client ID. Valid value is alphanumeric between 4 and 15 characters as specified by the Trading Partner on the Trading Partner Profile form.

Receiver ID: NEBRASKA MEDICAID'S ID Valid value is alphanumeric.
i.e. **MMISNEBR**

CORE Rule Version: The CORE Rule version 2.2.0 is used for this envelope.

Checksum: An element used to allow receiving site to verify the integrity of the message that is sent. Algorithm is SHA-1, encoding is Hex. Checksum must be computed only on the payload and not on the metadata (not applicable for retrieval request).

Payload: Payload contains compliant X12 270 request data or 276 request data. Payload should be encrypted using BASE 64 encode (not applicable for retrieval request).

Example:

```
--XbCY
Content-Disposition: form-data; name="PayloadType"
X12_999_SubmissionRequest_005010X231A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"
Batch
--XbCY
Content-Disposition: form-data; name="PayloadID"
f81d4fae-7dec-11d0-a765-00a0d91e6fa6
--XbCY Content-Disposition: form-data; name="PayloadLength"
10240
--XbCY Content-Disposition: form-data; name="TimeStamp"
2007-08-30T10:20:34Z
--XbCY Content-Disposition: form-data; name="SenderID"
YOURIDHERE
--XbCY Content-Disposition: form-data; name="ReceiverID"
```

MMISNEBR

```
--XbCY Content-Disposition: form-data; name="CORERuleVersion"
```

```
2.2.0
```

```
--XbCY Content-Disposition: form-data; name="Checksum"
```

```
6A3FE55946
```

```
--XbCY Content-Disposition: form-data; name="Payload"
```

```
SVNBKjAwKiAgICAqMDA=
```

```
--XbCY--
```

3.5 HTTP RESPONSES/ERROR MESSAGES

1. **HTTP 200 OK** – Returned when authentication is valid and request is accepted.
2. **HTTP 202 Accepted**– Returned when batch file submission has been accepted.
3. **HTTP 400 Bad Request** – Returned for incorrectly formatted HTTP headers.
4. **Server Errors** – When the real-time production system is not able to process a real-time request due to interface failures or other system unavailability, a standard 5xx series error such as “HTTP 500 Internal Server Error” or “HTTP 503 Service Error” will be returned by the application. Resubmission is recommended at a later time.

3.6 ENVELOPE RESPONSES/ERROR MESSAGES

1. **Success** – Envelope was processed successfully.
2. **<FieldName>Illegal** – Illegal value provided for <FieldName>.
3. **<FieldName>Required** – The field <FieldName> is required but was not provided.
4. **Version Mismatch** – The version of the envelope sent is not acceptable to the receiver. If the SOAP version is not valid at the receiver, a SOAP fault is returned with this fault code.
5. **Checksum Mismatched** – The checksum value computed on the recipient did not match the value that was sent in the envelope (not applicable for retrieval request).
6. **Unauthorized Error** – Invalid user name and password.

3.7 BATCH RESPONSE AND RETRIEVAL

All batch requests for eligibility, batch requests for 835 and batch results acknowledgment will be received by establishing a HTTP connection using CORE rules. The Trading Partners must submit a request for available responses.

4. PASSWORDS

A unique user ID and password will be assigned by NE Medicaid EDI Helpdesk and must be included when sending a transaction to Nebraska Medicaid.