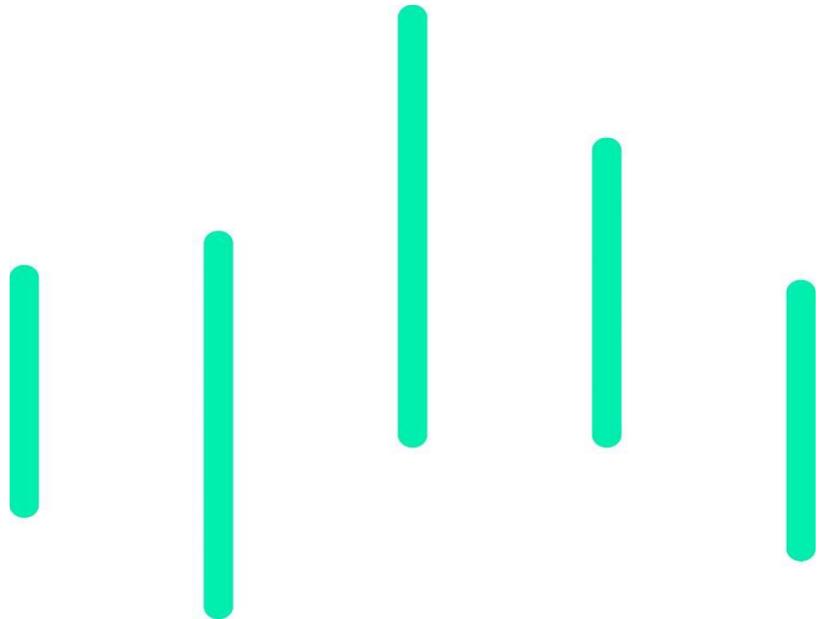




Colorado Medical Assistance Program Safe Harbor Real-time Vendor Interface Specifications



Version 1.0

Issue Date: 02/02/2026

Colorado Contract Number 14-64254

Submitted by: Gainwell Technologies

Gainwell Contract Number 2150458527

Table of Contents

| | |
|--|----|
| Introduction | 3 |
| Interface Standards..... | 3 |
| Web interface | 3 |
| Secure CORE Compliant Web Service..... | 4 |
| CORE Web Services..... | 4 |
| HTTP/S envelope standards..... | 4 |
| Functionality at a glance | 5 |
| Production vs. User Acceptance environments..... | 5 |
| Realtime processing mode | 6 |
| Connecting to the Server | 6 |
| RealTime Processing | 6 |
| Error Handling..... | 13 |
| HTTP level status | 13 |
| CORE envelope status/error codes and descriptions..... | 14 |
| Security Standards and Practices | 16 |
| Password creation requirements | 16 |
| Appendix A: Base64 encoding character set..... | 17 |
| Appendix B: CORE Service Types..... | 18 |
| Processing Modes..... | 18 |
| RealTime Payload Types..... | 18 |
| Modification Log..... | 19 |

Introduction

This document is intended for software vendors who wish to develop applications that interact with Colorado Medical Assistance Program file delivery and retrieval system. It was created and is maintained by Gainwell Technologies for the purpose of uploading and downloading Health Insurance Portability and Accountability Act (HIPAA) compliant transactions.

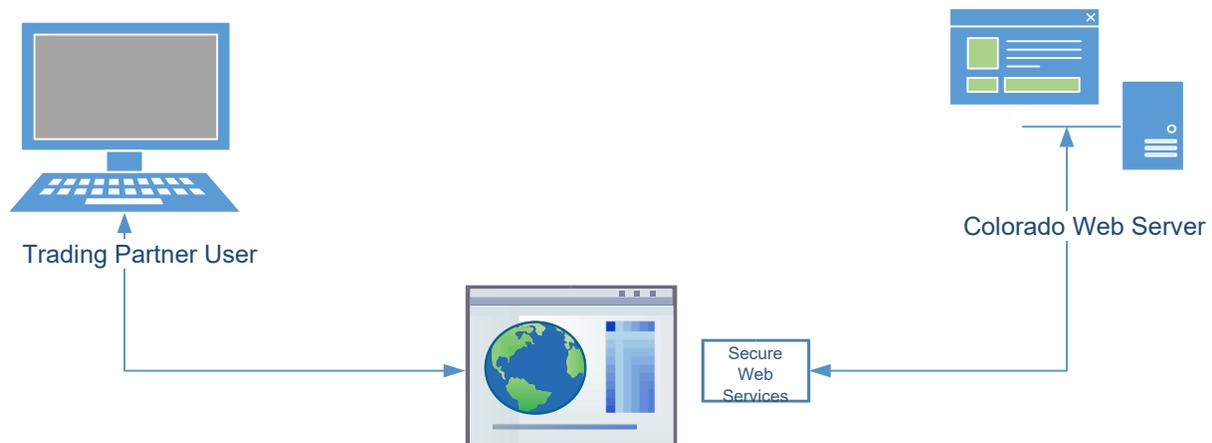
Interface Standards

Colorado Medical Assistance Program Safe Harbor interface supports the most used channel of communication, HTTP/S (web).

Web interface

Colorado Medical Assistance Program file delivery and retrieval system CORE compliant web interface is designed around CORE ACA 1104 Phase I and II rules, found at [CAQH CORE](#). This service is capable of accepting SOAP+WSDL. This service performs 270 and 276 real-time transactions. All data is transmitted using the Secure Socket Layer (SSL), which encrypts data over the network. Complete documentation can be found in the “CORE Web Service Specifications” section of this document.

The web interface is comprised of a CORE compliant interface capable of accepting real-time. A diagram of the interaction flow is below.



Secure CORE Compliant Web Service

CORE Web Services

The Colorado Medical Assistance Program's CORE compliant web services are also built around ACA 1104 Phase I and II rules which can be found at <https://www.cagh.org>.

WSDL, Data contracts, Security policies, application endpoints, and Colorado Medical Assistance Program-specific method definitions can be found on the Gainwell Technologies server at <https://colorado-coreservices.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime>.

HTTP/S Envelope Standards

Colorado Medical Assistance Program's CORE compliant web services are capable of accepting all Colorado-approved transactions from the following HTTP/S envelope standard: SOAP+WSDL. The envelope should conform to the CORE requirements listed below:

SOAP+WSDL

- HTTP/S version 1.1
- SOAP version 1.2
- WSDL version 1.1
- Web Service-Security 1.1
- CORE envelope version 2.2.0

Functionality Overview

HTTP/S supports a request-response message pattern, meaning that the sender must submit a message and wait for a response from the recipient. This usage pattern applies to batch and real-time ASC X12 transactions. The response message varies based on whether the sender's message was a real-time request, batch submission, or batch response retrieval request.

A list of the service functions can be seen below in Table 16. The functionality and CORE data envelope is inferred from the combination of processing mode and payload type. Request/response messages are described later in this guide.

Table 16 – SOAP+WSDL web methods

| Web Method | CORE | Supported |
|--|------|-----------|
| BatchSubmitTransaction | Yes | No |
| BatchSubmitAckRetrievalTransaction | Yes | No |
| BatchResultsRetrievalTransaction | Yes | No |
| BatchResultsAckSubmitTransaction | Yes | No |
| RealTimeTransaction | Yes | Yes |
| GenericBatchSubmissionTransaction | Yes | No |
| GenericBatchRetrievalTransaction | Yes | No |
| GenericBatchReceiptConfirmationTransaction | Yes | No |
| AdministrativeTransaction | No | No |

Production vs. User Acceptance Environments

The proper URL needs to be used to submit to the appropriate environment for processing each request based on the SenderID.

UAT

<https://colorado-coreservices-np.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime>

PROD

<https://colorado-coreservices-np.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime>

Realtime processing mode

Realtime requests should contain only a single inquiry, i.e., only one eligibility inquiry per single information source for a single patient. RealTime responses for the receipt of an ASC X12 270 or 276 will be returned within 20 seconds. The response will be an error response or the corresponding ASC X12 response (e.g., ASC X12 v5010 TA1, v5010 999, or v5010 271, if the request submitted was a v5010 270). All RealTime ASC X12 transaction data submitted or returned via SOAP 1.2 messaging standards should be sent in-line (within the SOAP message XML) as plain text that has been Base64 Encoded.

Connecting to the Server

Users can connect to the web service using a network connection that provides access to the public internet. The envelope standards used determine the application endpoint URL that will be used to connect to and interact with the Colorado Medical Assistance Program’s CORE services. Each interface listed below uses SSL version 3.0.

Realtime and administrative requests go to: [https://colorado-](https://colorado-coreservices.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime)

| Element | Description | Required |
|----------|--|----------|
| UserName | The submitter’s TPID. When using SOAP 1.2 messaging, the value is sent in the Username token of the security element within the SOAP header. | Y |

[coreservices.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime](https://colorado-coreservices.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime)

RealTime Processing

Realtime transactions may use the HTTP/S envelope standard covered in the previous sections. When using SOAP 1.2 messaging, the web method (seen in the “Functionality at Glance” section) will determine the appropriate CORE data envelope. All RealTime transactions must have a processing mode of *RealTime* and one of the acceptable RealTime payload types covered in Appendix I. An HTTP/S response containing a real-time CORE data envelope with an appropriate payload transactional response and an error code or description of envelope processing will be returned within 20 seconds. Consult the “Error Handling” section for more information regarding error situations. Descriptions of the RealTime CORE request and response data envelopes are listed in Tables 17 and 18.

RealTimeRequestMessage

Realtime transactions with the server should use a *RealTimeRequestMessage* comprised of an HTTP/S envelope and the RealTimeTransaction envelope as listed in Table 17. Only one ASC X12 envelope (ISA\IEA) containing a single inquiry may be submitted at a time and the total length in bytes of the entire message, including the HTTP/S envelope, must not exceed one (1) megabyte. If the message size exceeds this maximum, the entire request will be rejected. See Appendix J for a sample program.

Table 17 – COREEnvelopeRealTimeRequest description

| Element | Description | Required |
|----------------|--|----------|
| PassWord | <p>Type: String Sample: 12340001</p> <p>The submitter's password. When using SOAP 1.2 messaging, this value is in the Password token of the security element in the SOAP header. Password requirements can be found the "Security standards and Practices" section of this guide.</p> <p>Type: String Sample: 1qaz@WSX</p> | Y |
| PayloadType | <p>The type of data being sent in the payload. A list of acceptable payload types can be found in Appendix I.</p> <p>Type: String Sample: X12_270_Request_005010X279A1</p> | Y |
| ProcessingMode | <p>The mode in which the request should be processed. A list of acceptable PayloadTypes can be found in Appendix I.</p> <p>Type: String Sample: RealTime</p> | Y |
| PayloadID | <p>A unique identifier within the domain sending the request. A PayloadID may not be used more than once for a given ProcessingMode and SenderID combination.</p> <p>Type: UUID Sample: f81d4fae-7dec-11d0-a765-00a0c91e6bf6</p> | Y |

Sample XML and XML schema

Sample SOAP 1.2 RealTimeRequestMessage

```
POST https://colorado-coreservices.coxix.gainwelltechnologies.com/ACACoreService/CorerealTime HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/soap+xml;charset=UTF-8;action="http://tempuri.org/ICoreRealTime/RealTimeTransaction"
Content-Length: 2171
Host: colorado-coreservices.coxix.gainwelltechnologies.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.5.5 (Java/17.0.12)

<soap:Envelope xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd" xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:tem="http://tempuri.org/">
  <soap:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <wsse:UsernameToken wsu:Id="UsernameToken-4E75968BEE5466BC4417435478288201">
        <wsse:Username>xyz</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">abc</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <tem:RealTimeTransaction>
      <tem:Request>
        <cor:PayloadType>X12_270_Request_005010X279A1</cor:PayloadType>
        <cor:ProcessingMode>REALTIME</cor:ProcessingMode>
        <cor:PayloadID>TEST_COXIX</cor:PayloadID>
        <cor:TimeStamp>2020-06-12T12:31:08Z</cor:TimeStamp>
        <cor:SenderID>12566644</cor:SenderID>
        <cor:ReceiverID>COMEDASSISTPROG</cor:ReceiverID>
        <cor:CORERuleVersion>2.2.0</cor:CORERuleVersion>

        <cor:Payload>SVNBKjAwKiAglCAglCAglCAqMDAqICAglCAglCAglCpaWioxMjU2NjY0NCAGlCAglCAqWloqQ09NRURBU1NJU1RQUk9HKjIw
wMDYxMioxMjMxKl4qMDA1MDEqNzYyNDYwMTMwKjAqUCo6fg0KR1MqSFMqMTI1NjY2NDQqQ09NRURBU1NJU1RQUk9HKjIwMjAwNjEY
KjEYmzEqNzYyNDYwMTMwKlqgqMDA1MDEwWDI3OUExfg0KU1QqMjcwKjc2MjQ2MDEzMCowMDUwMTBYMjc5QTF+DQpCSFQqMDAyMio
xMyo3REM3NTMzMTI5N0ZGN0Y4MTIFNEQ3RDE2M0UzN0QqMjAyMDA2MTIqMTIzMX4NCkhMKjEgKjIwKjF+DQpOTTEqUFIqMipDT0xPU
kFETyBNRURJQ0FMIEFTU0ITVEFOQ0UgUFJPR1JBTSqKioqUEkqQ09fVfHJWH4NCkhMKjIqMSoyMSoxfg0Ktk0xKjFQKjIqVUNIkiqKipY
WCo3Nzc3Nzc3Nzd+DQpITCozKjIqMjIqMH4NCIRSTioxKjIwMjAwNjEYLTExNDk1OTAxKjIqQVNTUE9SVEh+DQpOTTEqSUwqMSoqKioqKk
1JKIhZWjEYmzR+DQpETUcqRDgqMjAyNTA4MjR+DQpEVFAqMjIxKjEJCoyMDI1MDQyMy0yMDI1MDQyM34NCkVRKjMwfg0KU0UqMTMq
NzYyNDYwMTMwfg0KR0UqMSo3NjI0NjAxMzB+DQpJRUEqMSo3NjI0NjAxMzB+DQo=</cor:Payload>
      </tem:Request>
    </tem:RealTimeTransaction>
  </soap:Body>
</soap:Envelope>
```

RealTimeResponseMessage

Table 18 – RealTimeTransactionResponsesdescription

| Element | Description | Require |
|-----------------|--|---------|
| PayloadType | An appropriate response payload type. A list of possible response payload types can be found in Appendix I. Type: String Sample: X12_271_Response_005010X279A1 | Y |
| ProcessingMode | The processing mode submitted in the request. Type: String Sample: RealTime | Y |
| PayloadID | The payload ID submitted in the request. Type: UUID Sample: f81d4fae-7dec-11d0-a765-00a0c91e6bf6 | Y |
| TimeStamp | The date and time, in UTC format, that the response was sent. Type: DateTime Sample: 2007-08-30T10:20:34Z | Y |
| SenderID | The ID of the sender. For all responses, this value must be 'COMEDASSISTPROG'. Type: String Sample: COMEDASSISTPROG | Y |
| ReceiverID | The ID of receiver. For all responses, this must match the TPID that submitted the request. Type: String Sample: 12340001 | Y |
| CORERuleVersion | The CORE envelope version being submitted. Colorado Medical Assistance Program only supports CORERuleVersion 2.2.0 Type: String Sample: 2.2.0 | Y |

| Element | Description | Require |
|--------------|--|---------|
| ErrorCode | The code of the error that occurred during message processing, not including ASC X12 transactional errors. This field will have a value of 'Success' when a successful transmission occurs. A list of possible error codes may be found in "Error Handling" section of this guide. Type: String Sample: Unauthorized | Y |
| ErrorMessage | A friendly description of the error code. This field will be empty when a successful transmission occurs. Type: String Sample: Invalid username/password or not allowed to sign on from this location | Y |
| Payload | The ASC X12 transactional response data. Returned in plain text Type: String Sample: ISA*00*W2540582 *00* *30*...IEA*1*000000031~ | Y |

Sample XML and XML schema

Sample SOAP RealTimeTransactionResponseMessage

```

HTTP/1.1 200 OK
Date: Fri, 24 Oct 2025 00:37:32 GMT
Content-Type: application/soap+xml; charset=utf-8
Connection: keep-alive
Set-Cookie:
AWSALB=WfOGivKm7OQCcAQqwrsmQBy+jJF6D2u/tcGIITPIGLOFgttITqMKEwPVLs2RgRXC2MXe1lhLLduwRvOa6gK+K6c7OJ3f1lBQ6weeVptTSP6dePGnykErqGovGjA; Expires=Fri, 31 Oct 2025 00:37:31 GMT; Path=/
Set-Cookie:
AWSALBCORS=WfOGivKm7OQCcAQqwrsmQBy+jJF6D2u/tcGIITPIGLOFgttITqMKEwPVLs2RgRXC2MXe1lhLLduwRvOa6gK+K6c7OJ3f1lBQ6weeVptTSP6dePGnykErqGovGjA; Expires=Fri, 31 Oct 2025 00:37:31 GMT; Path=/; SameSite=None; Secure
Server: Microsoft-IIS/10.0
Set-Cookie:
AWSALB=jru2oE9JnVdTzUpj1YBdY+fqL+n5KO46+arsSKyxrVMFMiXO6FhvFsTq5O24zUL7qPMuOS/F9bhUI97ovFBMIS5NKd77SI0+cHL+fDDIXAo6qhB6fp4e/Tbg6ka; Expires=Fri, 31 Oct 2025 00:37:31 GMT; Path=/
Set-Cookie:
AWSALBCORS=jru2oE9JnVdTzUpj1YBdY+fqL+n5KO46+arsSKyxrVMFMiXO6FhvFsTq5O24zUL7qPMuOS/F9bhUI97ovFBMIS5NKd77SIO+cHL+fDDIXAo6qhB6fp4e/Tbg6ka; Expires=Fri, 31 Oct 2025 00:37:31 GMT; Path=/; SameSite=None; Secure
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Powered-By: ASP.NET
Content-Length: 2881

```

```

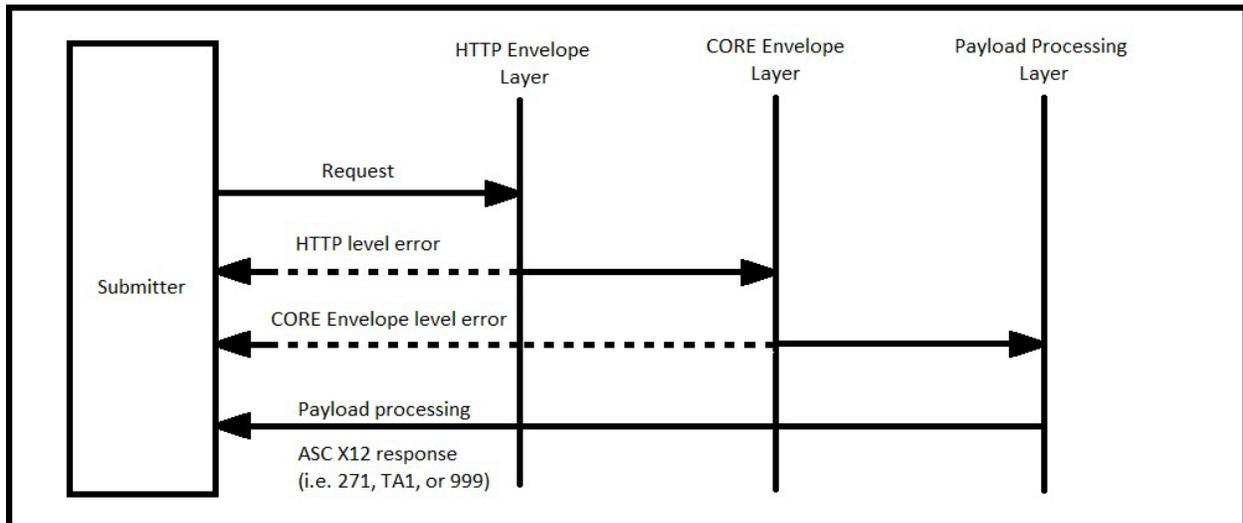
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"><s:Body><RealTimeTransactionResponse
xmlns="http://tempuri.org/"><RealTimeTransactionResult xmlns:a="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd"
xmlns:i="http://www.w3.org/2001/XMLSchema-
instance"><a:PayloadType>X12_271_Response_005010X279A1</a:PayloadType><a:ProcessingMode>REALTIME</a:Processing
Mode><a:PayloadID>TEST_COXIX</a:PayloadID><a:TimeStamp>2025-10-
24T00:37:31Z</a:TimeStamp><a:SenderID>COMEDASSISTPROG</a:SenderID><a:ReceiverID>12566644</a:ReceiverID><a:CO
RERuleVersion>2.2.0</a:CORERuleVersion><a:Payload>ISA*00*
*00*
*ZZ*COMEDASSISTPROG*ZZ*12566644
*251023*2037*^*00501*600656965*0*P*~GS*HB*COMEDASSISTPROG*12566644*20251023*203732*600656965*X*005010X27
9A1~ST*271*762460130*005010X279A1~BHT*0022*11*7DC75331297FF7F819E4D7D163E37D*20251023*2037~HL*1**20*1~N

```

M1*PR*2*COLORADO MEDICAL ASSISTANCE
PROGRAM*****PI*CO_TXIX~HL*2*1*21*1~NM1*1P*2*UCH*****XX*77777777~HL*3*2*22*0~TRN*1*252960VHJW*1811725341~
TRN*2*20200612-11495901*9PASSPORTH~NM1*IL*1*LNAME*FNAME*M***MI*XYZ1234~REF*SY*999999999~N3*1222 EASY
STREET~N4*DENVER*CO*802050000~DMG*D8*20250824*F~INS*Y*18*001*25~DTP*291*RD8*20250423-
20250423~EB*MC*IND**HM*Administrative Service Organization - Dental~DTP*307*RD8*20250423-
20250423~MSG*MCSTARTRSN\$97 - System Assigned - Conversion Start~LS*2120~NM1*13*2*DENTAQUEST USA INSURANCE
CO IN*****SV*16374576~PER*IC**TE*8552251729~LE*2120~EB*MC*IND**HM*REGIONAL ACCOUNTABLE
ENTITY~DTP*307*RD8*20250423-20250423~MSG*MCSTARTRSN\$10 - Enrollment Broker - Stop
Reason~LS*2120~NM1*13*2*COLORADO COMMUNITY HEALTH
ALLI*****SV*99999906~PER*IC**TE*8556274685~LE*2120~EB*L*IND**HM*Primary Care Medical
Provider~DTP*307*RD8*20250423-20250423~MSG*MCSTARTRSN\$01 - Client
Requested|MCD\$48638579~LS*2120~NM1*13*2*KP LAKEWOOD MEDICAL
OFFICES*****XX*1588778211~PER*IC**TE*3033383800~LE*2120~EB*D*CHD*81*MC*EPSDT-
Medical~DTP*304*D8*20251016~DTP*356*D8*20261016~EB*D*CHD*35*MC*EPSDT-
Dental~DTP*304*D8*20250816~DTP*356*D8*20260216~EB*D*CHD*77*MC*EPSDT- Hearing~EB*D*CHD*AL*MC*EPSDT-
Vision~EB*D*CHD*9*MC*EPSDT- Other~EB*1*IND*47^48^50^86^98^MH^30*MC*Medicaid Behavioral Health Benefits -
70~DTP*307*RD8*20161201-22991231~MSG*COPAYSTATUS\$COPAYEXEMPT~EB*B*IND*47^48^50^86^98^MH*MC*Medicaid
Behavioral Health Benefits - 70**0~EB*1*IND*1^33^35^88^91^92^AL^UC*MC*Medicaid Behavioral Health Benefits -
70~DTP*307*RD8*20161201-22991231~EB*1*IND*1^35^47^48^50^86^88^91^92^98^AL^MH^UC^30*MC*Medicaid State Plan -
70~DTP*307*RD8*20161201-
22991231~MSG*COPAYSTATUS\$COPAYEXEMPT~EB*B*IND*1^35^47^48^50^86^91^92^98^AL^MH^UC*MC*Medicaid State
Plan - 70**0~EB*1*IND*33*MC*Medicaid State Plan - 70~DTP*307*RD8*20161201-
22991231~SE*59*762460130~GE*1*600656965~IEA*1*600656965~</a:Payload><a:ErrorCode>Success</a:ErrorCode><a:ErrorM
essage/></RealTimeTransactionResult></RealTimeTransactionResponse></s:Body></s:Envelope>

Error Handling

The error handling layers described in this section is applicable to the HTTP/S envelope standards. Each request made to the Colorado Medical Assistance Program’s CORE services goes through three (3) logical layers and if an error occurs at one of those logical layer (envelope only), then an error response will be returned. If an envelope passes validation and the payload makes it to the payload processor, then the appropriate response (ASC X12 or Colorado payload results) will indicate the outcome of processing.



Note: The dashed lines represent error messages returned if an error occurs at the corresponding processing layer. The solid lines represent request/response messages.

HTTP Level Status

The following HTTP status codes situations apply to *RealTime*:

- HTTP 200 OK
 - The submitted request passed HTTP envelope validation. However, CORE envelope validation may have failed. Check the CORE response envelope for possible errors. If no error is detected, the request was successful.
- HTTP 400 Bad Request
 - HTTP envelope headers or MIME parts are malformed, check the response for likely causes.
 - When using SOAP messaging and the response is empty. Most likely, the message could not be properly routed. Check the SOAP action headers.
- HTTP 403 Forbidden
 - The submitted request passed HTTP envelope validation but failed authentication of submitted credentials.
- HTTP 500 Internal Error
 - A message is received, but an internal process failed (e.g. batch or real-time services are down). Check the response for either: SOAP fault code “Receiver”, in the case of SOAP messaging, or a CORE envelope error code “Receiver”, in the case of MIME Multi-part messaging.

- If no response message is contained in the HTTP response envelope, the message was most likely not received or was rejected at the server level. A likely cause of this is an invalid SOAP version (SOAP messaging only). Check the media type HTTP header for an “Unsupported media type” condition.
- HTTP 503 Service Unavailable
 - CORE web services are down.

CORE envelope status/error codes and descriptions

| Element | Description |
|--------------------------|---|
| Success | The message was processed successfully. |
| <FieldName>Illegal | The value provided for <FieldName> is valid. |
| <FieldName>Required | The field <FieldName> is required but was not provided. |
| <FieldName>NotUnderstood | The field <FieldName> is not understood at the receiver. In the case of SOAP, this error is returned as a “NotUnderstood SOAP” fault. |
| VersionMismatch | The version on CORE envelope is not acceptable. |
| Unauthorized | The username/password supplied is not authorized |
| ChecksumMismatched | The checksum computed on the payload by the receiver did not match the checksum sent by the client. |
| Sender | The CORE envelope sent by the sender contained data that was legal but could not be processed for some reason (e.g., duplicate PayloadID, password strength when changing password, use of unsupported CORE web methods). |
| Receiver | The message could not be processed for some reason attributable to the receiver (e.g., upstream process not available). In the case of SOAP, this error will be returned in a SOAP fault with fault code “Receiver”. |

Reserved

Security Standards and Practices

In order for Gainwell Technologies to guarantee a safe and stable working environment, the following security standards and practices have been established. These measures protect users and Gainwell Technologies from potential threats.

Password creation requirements

Passwords must contain:

- A minimum of 8 alpha-numeric-special characters
- At least 1 upper and 1 lower case alpha character
- At least 1 number
- At least 1 special character Passwords **cannot**:
 - Be similar to username (TPID)
 - Use any common 'dictionary' words
 - Use previous six (6) passwords

Appendix A: Base64 encoding character set

The base64 encoding/decoding character set is a widely accepted standard; in ascending order from zero are the uppercase characters "A" to "Z", the lowercase characters "a" to "z", the numerals "0" to "9", and the symbols "+" and "/". The valueless character "=" is used for trailing padding.

Appendix B: CORE Service Types

Processing Modes

- RealTime

RealTime Payload Types

Request PayloadTypes

- X12_270_Request_005010X279A1
- X12_276_Request_005010X212 Response PayloadTypes
- X12_271_Response_005010X279A1
- X12_277_Response_005010X212

Modification Log

| Rev # | Date | Author | Section | Nature of Change |
|-------|------------|-----------------------|---------|--|
| 1.0 | 02/02/2026 | Gainwell Technologies | | Initial Creation of Safe Harbor Core Interface Guide |