BlueCross BlueShield of Tennessee

ASC X12N 276/277 (005010X212)
Health Care Claim Status Request and Response
BlueCORE Phase II System Companion Guide
Version 2.0

November 2011

Disclosure Statement

The information in this document is subject to change. Changes will be posted via the BlueCross BlueShield of Tennessee website located at http://www.bcbst.com/providers/ecomm/ as well as http://bluecore.bcbst.com/.

THE 277 RESPONSE RETURNED BY BLUECROSS BLUESHIELD OF TENNESSEE SHOULD NOT BE INTERPRETED AS A GUARANTEE OF PAYMENT. PAYMENT OF BENEFITS REMAINS SUBJECT TO ALL HEALTH BENEFIT PLAN TERMS, LIMITS, CONDITIONS, EXCLUSIONS AND THE MEMBER'S ELIGIBILITY AT THE TIME SERVICES ARE RENDERED.

Preface

The Health Insurance Portability and Accountability Act (HIPAA) requires health insurance payers and covered entities in the United States to comply with the EDI standards for health care as defined in the ASC X12N Implementation Guides.

The following information is intended to serve as a companion document to the HIPAA ASC X12N 276/277 (005010X212) Implementation Guide for Claim Status Inquiry. The use of this document is solely for the purpose of clarification on usage of the BlueCORE solution.

The information describes specific requirements for submitting claim status inquiry requests for BlueCross BlueShield of Tennessee members through BlueCORE. BlueCORE is BlueCross BlueShield of Tennessee's "CORE Certified" solution, providing eligibility, benefits, and claim status information.

This companion document supplements, but does not exceed any requirements in the ASC X12N 276/277 (005010X212) Implementation Guide.

Table of Contents

1. INTRODUCTION

This application for real-time and batch 276/277's follows the CAQH/CORE Phase II guidelines.

1.1 Scope

Providers, billing services and clearinghouses are advised to use the ASC X12N 276/277 (005010X212) Implementation Guide as a basis for their submission of Claim Status inquires. This companion document should be used to clarify the CORE Business rules for 276/277 data content requirements, batch and real-time acknowledgment, connectivity, response time, and, system availability, specifically for submissions through the BlueCORE system. These rules differ from the Companion Guide for submissions via BlueCross BlueShield of Tennessee's ECGateway connection. This document is intended for use with CAQH CORE compliant systems. For additional information on building a CORE compliant system go to http://www.caqh.org.

1.2 Overview

The purpose of this document is to introduce and provide information about BlueCross BlueShield of Tennessee's CAQH/CORE certified solution for submitting real-time 276/277 transactions.

1.2.1 What is CAQH?

CAQH stands for The Council for Affordable and Quality Healthcare. It is a not-for-profit alliance of health plans, provider networks, and associations with a goal to provide a variety of solutions to simplify health care administration.

1.2.2 What is CORE?

The Committee on Operating Rules for Information Exchange (CORE) is a multi-stakeholder initiative created, organized and facilitated by CAQH. CORE's Phase II goal is to create, disseminate, and maintain operating rules that enable health care providers to quickly and securely obtain reliable health care eligibility and benefits information. CORE operating rules will decrease the amount of time and resources providers spend verifying patient eligibility, benefits and other administrative information at the point of care. CORE operating rules, envisioned to be introduced in multiple phases, have support from health plans, medical professional societies, providers, vendors, associations, regional entities, standard setting organizations, government agencies and other health care constituencies.

1.2.3 What is CAQH/CORE certification?

Any entity that creates, transmits, or uses eligibility or claim status data is eligible to become CORE-certified. CORE-certification indicates an entity has signed the CORE Pledge and successfully completed certification testing, both of which are designed to demonstrate an entity's compliance with all the CORE Phase II rules. Any entity that agrees to follow the CORE operating rules will be expected to exchange eligibility and benefits information per the requirements of the CORE Phase II rules and policies, with all its trading partners. Given the requirements of the CORE Phase II rules, use of these rules by the industry will enhance the usability and content of the eligibility and claim status transaction as well as decrease administrative costs and resources. See http://www.caqh.org/.

1.3 References

1.3.1 ASC X12 Version 5010A1 Implementation Guides: http://www.wpc-edi.com

1.3.2 BCBST BlueAccess: http://www.bcbst.com/blueaccess/

1.3.3 CAQH/CORE: http://www.caqh.org/benefits.php

1.3.4 WSDL: http://www.w3.org/TR/wsdl

1.3.5 SOAP: http://www.w3.org/TR/soap/

1.3.6 MIME Multipart: http://www.w3.org/Protocols/rfc1341/7_2_Multipart.html

1.3.7 CORE XML Schema: http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd

1.4 Additional Information

Submitters must have Internet (HTTPS) connection capability to submit a CORE 276 request and receive 277 responses.

Submitters must possess a valid BlueAccess user ID and password in order to submit inquiries through the BlueCORE option.

The submitter must be associated with at least one provider in the BlueCross BlueShield of Tennessee provider database.

Both real-time and batch 276 inquiries are supported.

This system supports inquiries for BlueCross BlueShield of Tennessee members only.

2. GETTING STARTED

2.1 Working with BlueCross BlueShield of TN

Providers, billing services and clearinghouses interested in submitting 276 inquiries and receiving 277 responses via BlueCross BlueShield of Tennessee's CORE Certified Solution should contact BlueCross BlueShield of Tennessee at (423) 535-5717, Monday through Friday, 8 a.m. to 6:30 p.m. (ET).

2.2 Trading Partner Registration

Trading Partner Registration is not required in order to submit BlueCORE 276 requests.

2.3 Certification and Testing Overview

BlueCross BlueShield of Tennessee recommends submitting at least one test file to ensure connectivity and data transfer is successful. The testing link is below:

HTTP Request:
https://beta-bluecore.bcbst.com/caqh/realtime

SOAP Request:
https://beta-bluecore.bcbst.com/caqh/Core

3. TESTING WITH THE PAYER

Listed below are steps to follow when testing:

- Register for BlueAccess user ID and password (only if user does not already have a valid BlueAccess user ID)
- Create test transaction based on Companion Guide/Implementation Guide specifications
- Submit via the testing link, either Real-Time or Batch
- Retrieve appropriate response (TA1, 999, 277)
- Review response to determine production readiness

4. CONNECTIVITY / COMMUNICATIONS

Blue CORE System Availability

Monday-Sunday 3 a.m.-2 a.m. (following day)

(system maintenance from 2:01 a.m.-2:59 a.m.)

Thursday (system maintenance 7p.m.–10 p.m.)

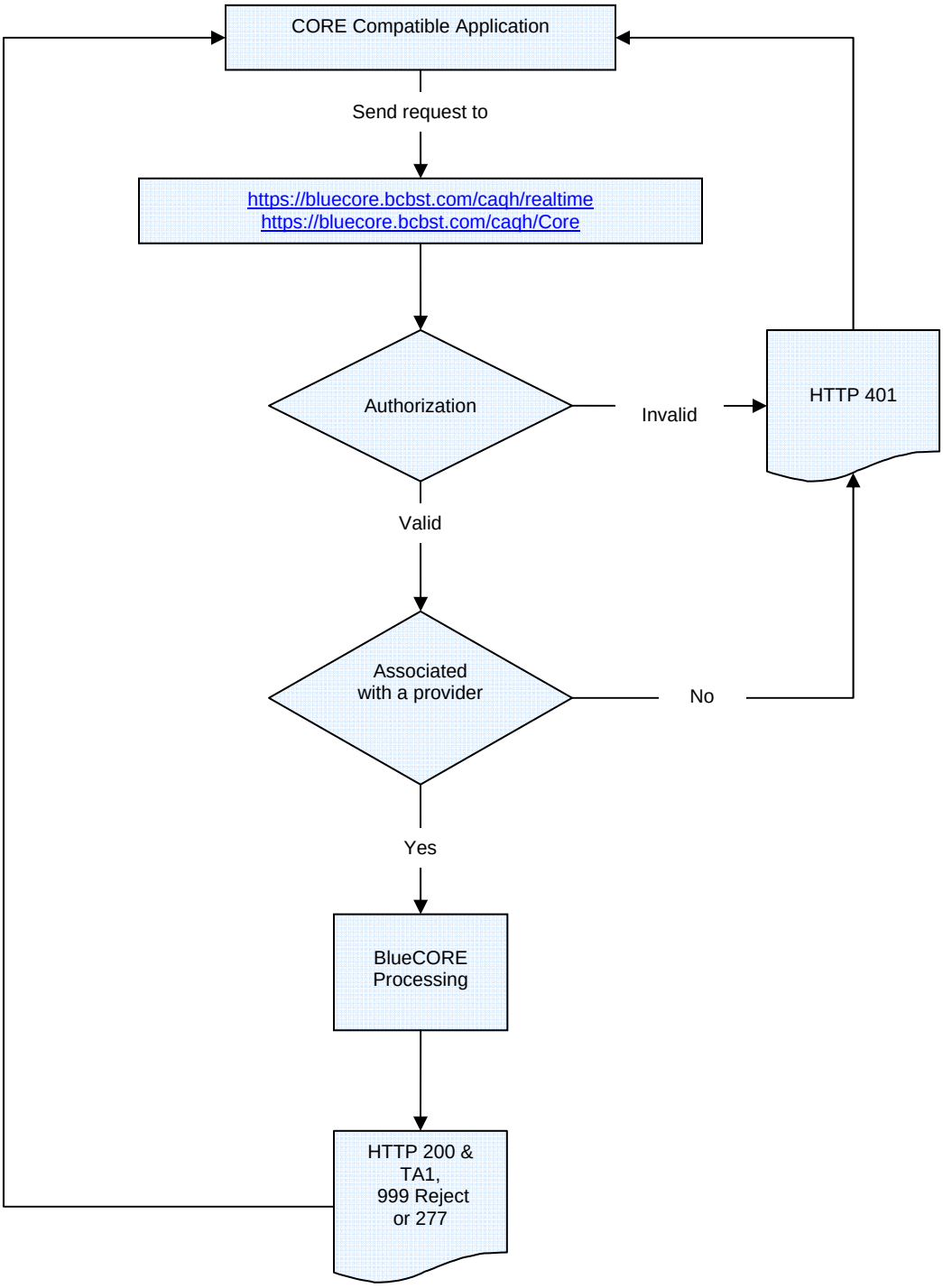
Please refer to the BlueCORE Splash page https://bluecore.bcbst.com/ for the most up-to-date information on system availability. All scheduled downtimes will be posted and emergency downtimes will be reflected.

4.1 Process Flows

4.1.1 Real-time

- The user application submits an HTTPS request to: https://bluecore.bcbst.com/caqh/realtime
- The user application submits an SOAP request to: https://bluecore.bcbst.com/caqh/Core
- The BlueCORE system authenticates the user and ensures the user has been associated with at least one provider in the BlueCross BlueShield of Tennessee provider database. If the user is not authorized, or is authorized but not associated with at least one BlueCross BlueShield of Tennessee provider number, then an HTTP 401 Unauthorized response is returned.
- If the user is successfully authorized, an HTTP 200 OK status response will be returned to the user within 20 seconds and the following files will be issued:
    - TA1 (if problem with the ISA/IEA segments exist)
    - 999 Reject (if problem occurs within the subsequent loops and segments)
    - 277 Eligibility Response

Below is an example of a real-time submission:

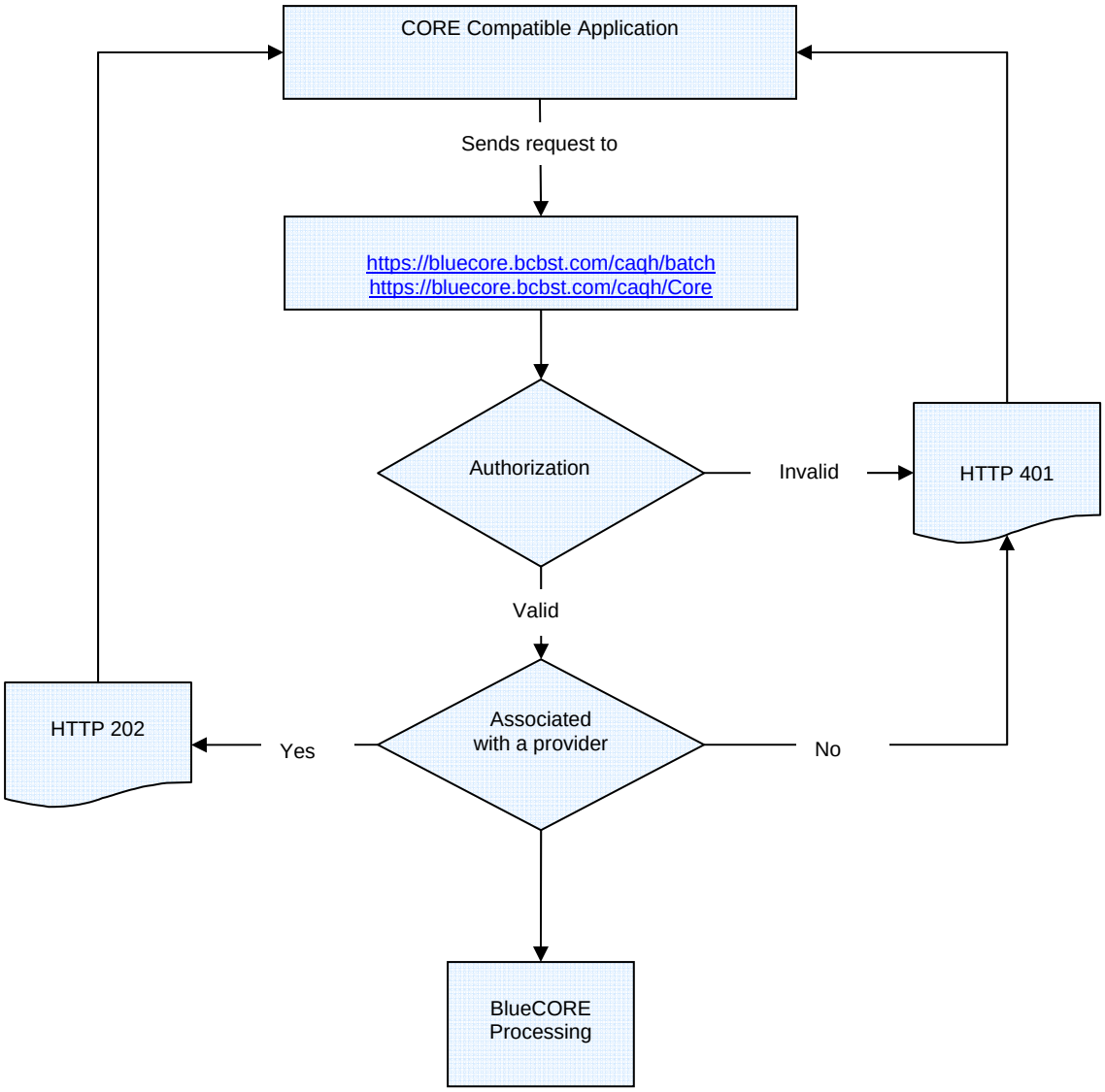


4.1.2 Batch

4.1.2.1 Submission

- The user application submits an HTTPS request to: https://bluecore.bcbst.com/caqh/batch
- The user application submits an SOAP request to: https://bluecore.bcbst.com/caqh/Core
- The BlueCORE system authenticates the user and ensures the user has been associated with at least one provider in the BlueCross BlueShield of Tennessee provider database. If the user is not authorized, or is authorized but not associated with at least one BlueCross BlueShield of Tennessee provider number, then an HTTP 401 Unauthorized response is returned.
- If the user is successfully authorized, an HTTP 202 OK status is returned to the user indicating BlueCross BlueShield of Tennessee has accepted the batch transaction for processing.
- A response to the batch submission will be available by 7 a.m. the following day. Batch requests submitted after 9 p.m. (ET) will be available by 7 a.m. two days following submission.

Below is an example of a batch submission:



4.1.2.2 Pickup

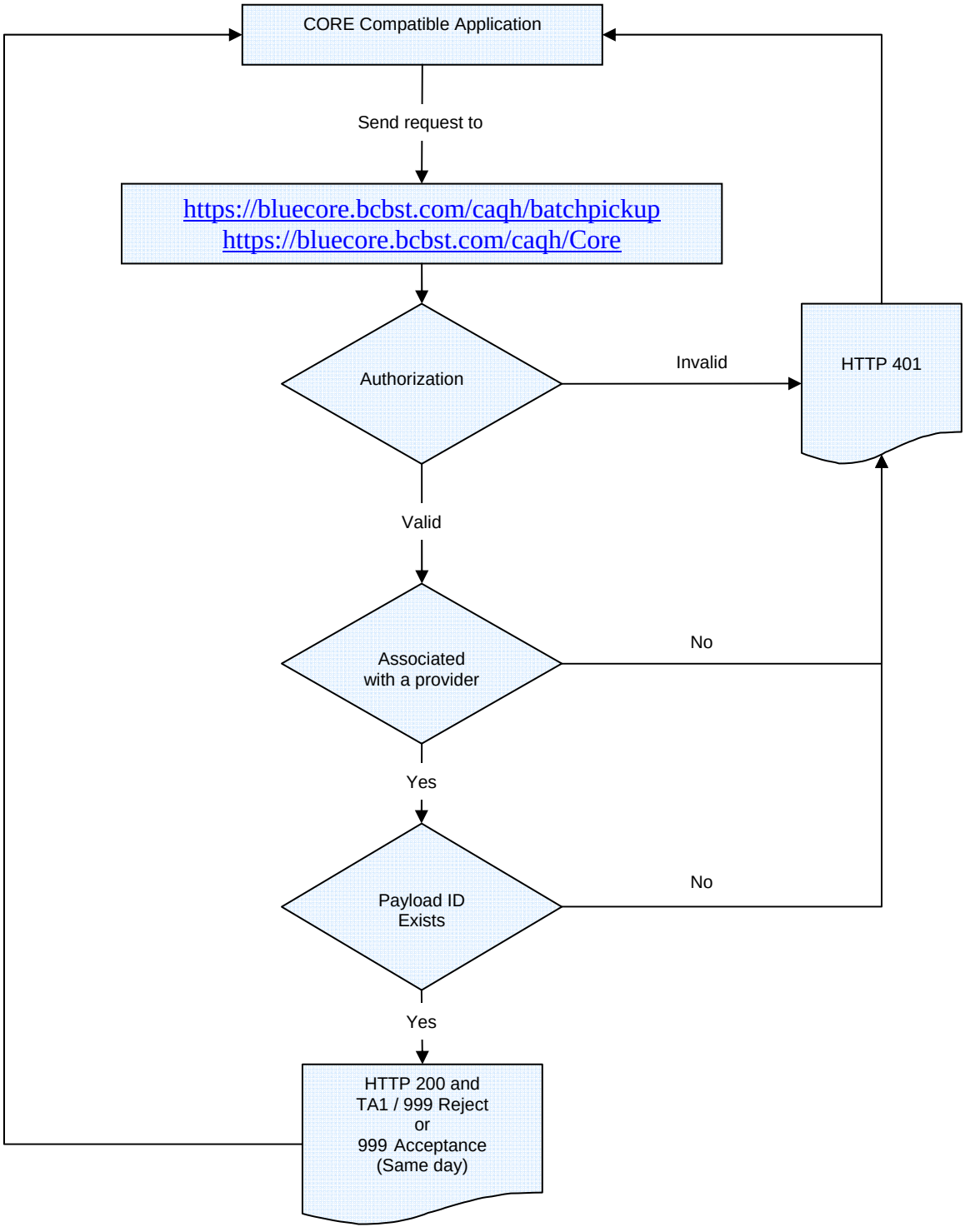
- The user submits an HTTPS / SOAP pick-up request* using the Payload ID to: https://bluecore.bcbst.com/caqh/batchpickup https://bluecore.bcbst.com/caqh/Core
- The Blue CORE system authenticates the user and ensures the user has been associated with at least one provider in the BlueCross BlueShield of Tennessee provider database. If the user is not authorized, or is authorized but not associated with at least one BlueCross BlueShield of Tennessee provider number, then an HTTP 401 Unauthorized response is returned.
- If the user is successfully authorized, one of the following will be generated back to the user:
    - TA1 available within one hour, if there is a problem with the ISA or IEA segments
    - 999 Reject available within one hour, if there is a problem with the segments occurring between the ISA and IEA.
    - 999 Acceptance response will be available within one hour.
    - The 277 transaction(s)** will be available the following day (no later than 7:00a.m.).***

** There should be NO file attached to the batch pickup request form.*

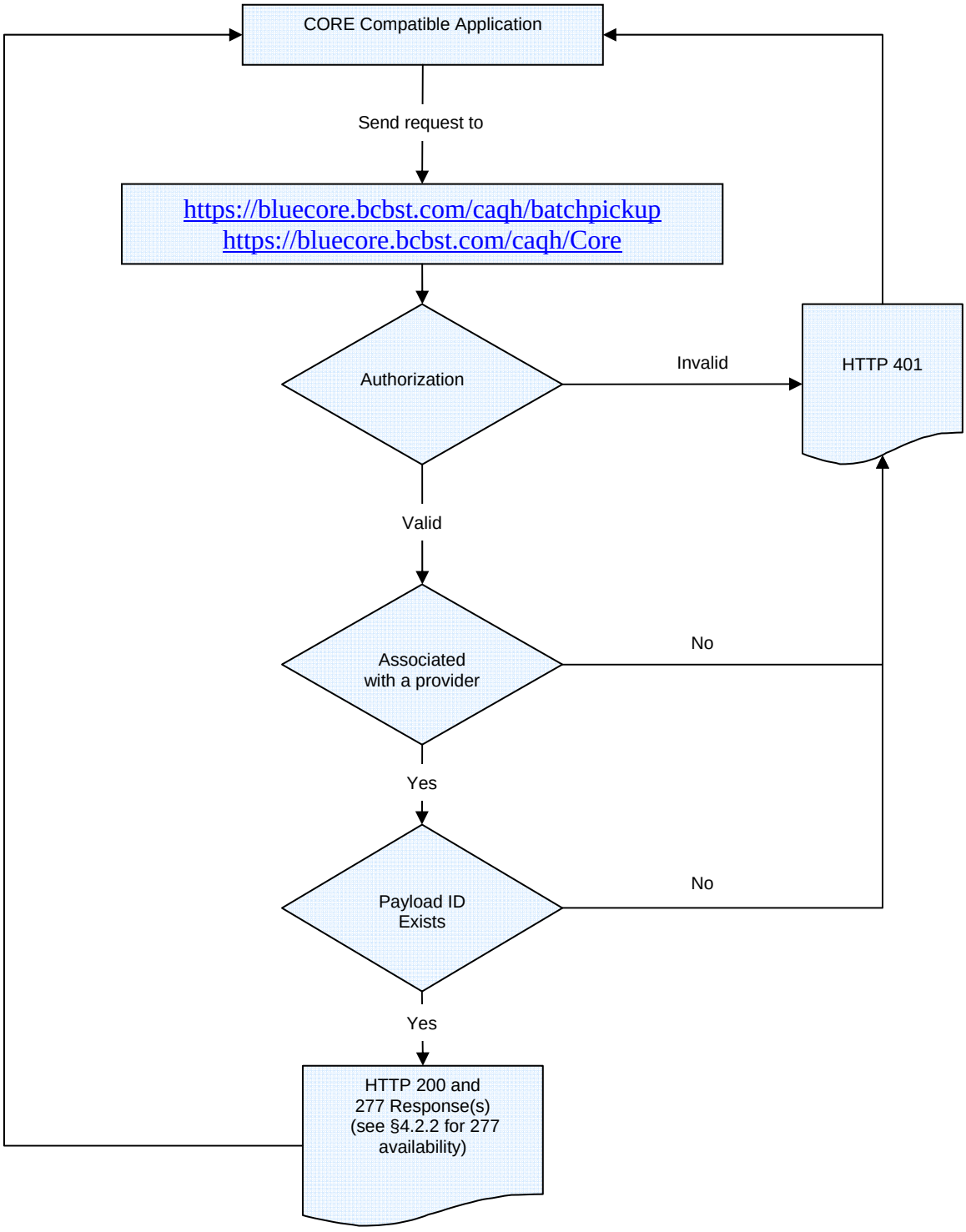
*** The 277 batch response file may contain a single or multiple 277 transactions. In Blue CORE batch transmissions, each 276 must be enveloped in its own ST-SE segment. There will be a 277 response for every occurrence of ST-SE segments in the file*.

****All 999s and 277s will be available for retrieval for at least 30 days.*

Below is an example a batch TA1 / 999 acknowledgement pickup request:



Below is an example of a 277 batch pickup request:



4.2 Transmission Administrative Procedures

4.2.1 Structure Requirements

Real-time 276 requests are limited to one inquiry, per patient, per transaction.

Batch 276 requests are limited to **99** ST/SE groupings per transaction. Each batch inquiry **must** be in its own ST/SE.

4.2.2 Response Times

A response (TA1, 999 reject or 277) to real-time inquiries will be provided within **20 seconds***.

A response to the batch inquiry will be provided by **7 a.m. (ET) the following day**. Batch requests submitted **after 9 p.m. (ET)** will be available by **7 a.m. (ET) *two* days following submission**.

Due to requirements from the BlueCross BlueShield Association, transactions that must be sent to other BCBS plans for processing (BlueCard/FEP) may take up to **45 seconds to generate a response.*

4.3 Re-transmission Procedures

If the HTTP post reply message is not received within the 60-second response period, the user's CORE compliant system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

If no response is received after the second attempt, the user's CORE compliant system should submit no more than five duplicate transactions within the next 15 minutes. If the additional attempts result in the same timeout termination, the user's CORE compliant system should notify the user to contact the health plan or information source directly to determine if system availability problems exist or if there are known Internet traffic constraints causing the delay.

4.4 Communication Protocols

4.4.1 HTTP MIME Multipart

BlueCORE supports standard HTTP MIME messages. The MIME format used must be that of *multipart/form-data*. Responses to transactions sent in this manner will also be returned as *multipart/form-data*.

4.4.1.1 Header Requirements

The HTTP header requirements for MIME transactions are as follows:

- UserName (8 character max)
- ProcessingMode
  - Accepted values are:
    - RealTime - for real time inquiries
    - Batch - for batch inquiries (either submission or pickup)
- Password (50 character max)
- PayloadType
  - Accepted values are:
    - X12_276_Request_005010X212
      - Real-time & Batch Submission
    - X12_005010_Request_Batch_Results_277
      - Batch Results Retrieval
    - X12_005010_Request_BatchSubmissionMixed
      - Mixed batch
    - X12_005010_Request_BatchResultsMixed
      - Mixed Batch Pickup
    - X12_TA1_SubmissionRequest_00501X231A1
      - TA1 pickup (Batch)
    - X12_999_RetrievalRequest_005010X231A1
      - 999 Pickup (Batch)
- PayloadID
  - Should conform to ISO UUID standards (described at ftp://ftp.rfceditor.org/in-notes/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address35, to ensure uniqueness.
- SenderID (50 character max)
- CORERuleVersion
  - Accepted value is:
    2.2.0
- ReceiverID (50 character max)
- Payload
  - This contains the X12 request
- PayloadLength
  - Length of the X12 document, required only if ProcessingMode is Batch
- CheckSum
  - Checksum of the X12 document, using SHA-1; encoding is hex; required only if ProcessingMode is Batch
- TimeStamp
  - In the form of YYYY-MM-DDTHH:MM:SSZ; see http://www.w3.org/TR/xmlschema11-2/#dateTime

- Envelope – Errors regarding the structure or data included within the body of the MIME multipart message will be reported at this level in a response of type *multipart/form-data*.
    - Success -- no errors
    - PayloadIDRequired -- missing PayloadID
    - UserNameRequired -- missing UserName
    - PasswordRequired -- missing Password
    - PayloadRequired -- missing Payload
    - SenderIDRequired -- missing SenderID
    - ReceiverIDRequired -- missing ReceiverID
    - CORERuleVersionRequired -- missing CORERuleVersion
    - VersionMismatch -- CORERuleVersion is not supported
    - Receiver -- unexpected error during processing
    - PayloadIDIllegal -- duplicate PayloadID sent by client
    - UnAuthorized -- username/password was not found
    - ChecksumMismatched – SHA-1 checksum invalid (batch only)
- Transaction (X12) – Errors regarding ANSI transaction compliancy will be returned as a MIME multipart/form-data message containing the related ANSI response data, i.e. TA1 or 999.

4.4.1.2 Error Reporting

There are 3 levels of error validation involved in a BlueCORE MIME multipart transaction:

- HTTP – Errors with connectivity, authorization, etc, will be reported at this level.
    - HTTP 200 OK – no errors
    - HTTP 202 Accepted – batch submission accepted
    - HTTP 400 Bad Request – error with HTTP header
    - HTTP 401 Unauthorized – username/password invalid
    - HTTP 500 Internal Server error -- unexpected error during processing

- Envelope – Errors regarding the structure or data included within the body of the MIME multipart message will be reported at this level in a response of type *multipart/form-data*.
    - Success -- no errors
    - PayloadIDRequired -- missing PayloadID
    - UserNameRequired -- missing UserName
    - PasswordRequired -- missing Password
    - PayloadRequired -- missing Payload
    - SenderIDRequired -- missing SenderID
    - ReceiverIDRequired -- missing ReceiverID
    - CORERuleVersionRequired -- missing CORERuleVersion
    - VersionMismatch -- CORERuleVersion is not supported
    - Receiver -- unexpected error during processing
    - PayloadIDIllegal -- duplicate PayloadID sent by client

  - UnAuthorized -- username/password was not found
  - ChecksumMismatched – SHA-1 checksum invalid (batch only)
- Transaction (X12) – Errors regarding ANSI transaction compliancy will be returned as a MIME multipart/form-data message containing the related ANSI response data, i.e. TA1 or 999.

4.4.1.3 Submission / Retrieval

4.4.1.3.1 Real-time

Real-time requests sent to the BlueCORE system must be submitted to the following URL:

https://bluecore.bcbst.com/caqh/realtime

4.4.1.3.2 Batch

Batch requests sent to the BlueCORE system must be submitted to the following URL:

https://bluecore.bcbst.com/caqh/Core

4.4.1.4 Examples

Below is an example of a HTTP MIME Multipart submission:

```
POST /core/claimstatus HTTP/1.1
Host: server_host:server_port
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY
--XbCY
Content-Disposition: form-data; name=“PayloadType“
X12_276_Request_005010X212
--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=“UserName"
hospa
--XbCY
Content-Disposition: form-data; name=“Password"
8y6dt3dd2
--XbCY
Content-Disposition: form-data; name=“SenderID"
HospitalA
--XbCY
Content-Disposition: form-data; name=“ReceiverID"
PayerB
--XbCY
Content-Disposition: form-data; name=“CORERuleVersion"
```

```
2.2.0
--XbCY
Content-Disposition: form-data; name="Payload"
<contents of file go here -- 1674 bytes long as specified above>
--XbCY—
```

Below is an example of a response:

```
HTTP/1.1 200 OK
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY
--XbCY
Content-Disposition: form-data; name="PayloadType"
X12_277_Response_005010X212
--XbCY
Content-Disposition: form-data; name="ProcessingMode"
RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"
f81d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"
2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="SenderID"
PayerB
--XbCY
Content-Disposition: form-data; name="ReceiverID"
HospitalA
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"
2.2.0
--XbCY
Content-Disposition: form-data; name="ErrorCode"
Success
--XbCY
Content-Disposition: form-data; name="ErrorMessage"
None
--XbCY
Content-Disposition: form-data; name="Payload"
<contents of file go here -- 1674 bytes long as specified above>
--XbCY--
```

4.4.2 SOAP + WSDL

BlueCORE also supports transactions formatted according to the *Simple Object Access Protocol* (SOAP) conforming to standards set forth by the *Web Services Description Language* (WSDL) for XML envelope formatting, submission, and retrieval.

4.4.2.1 SOAP XML Schema

The XML schema definition set forth by CORE and used in BlueCORE is located at:

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

This file contains definitions for each type of request or response accepted or sent by BlueCORE.

4.4.2.2 WSDL Information

The WDSL definition set forth by CORE and used in BlueCORE is located at:

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

This file conforms to the XML schema set forth in §4.4.2.1 and contains definitions for each message and transaction type accepted by BlueCORE.

4.4.2.3 SOAP Version Requirements

BlueCORE requires that all SOAP transactions conform to SOAP Version 1.2.

4.4.2.4 Error Reporting

There are 3 levels of error validation involved in a BlueCORE SOAP transaction:

- HTTP – Errors with connectivity, authorization, etc, will be reported at this level.
  - HTTP 200 OK – no errors
  - HTTP 202 Accepted – batch submission accepted
  - HTTP 400 Bad Request – error with HTTP header
  - HTTP 401 Unauthorized – username/password invalid
  - HTTP 500 Internal Server error -- unexpected error during processing
- Envelope -- Errors regarding the structure or data included within the body of the SOAP message, respective to the definitions set forth in the SOAP fault specifications, located at http://www.w3.org/TR/soap12-part1/#soapfault. Application specific errors are as follows:
  - Success -- no errors
  - PayloadIDRequired -- missing PayloadID
  - UserNameRequired -- missing UserName
  - PasswordRequired -- missing Password
  - PayloadRequired -- missing Payload
  - SenderIDRequired -- missing SenderID
  - ReceiverIDRequired -- missing ReceiverID
  - CORERuleVersionRequired -- missing CORERuleVersion
  - VersionMismatch -- CORERuleVersion is not supported
  - Receiver -- unexpected error during processing
  - PayloadIDIllegal -- duplicate PayloadID sent by client
  - UnAuthorized -- username/password was not found
  - ChecksumMismatched – SHA-1 checksum invalid (batch only)
- Transaction (X12) -- Errors regarding ANSI transaction compliancy will be returned as a SOAP message containing the related ANSI response data, i.e. TA1 or 999.

4.4.2.5 Submission / Retrieval

Detailed SOAP+WSDL envelope standard for CORE Phase II Connectivity can be found at http://www.caqh.org/pdf/CLEAN5010/270-v5010.pdf.

4.4.2.5.1 Real-time

Real-time requests sent to the BlueCORE system must be submitted to the following URL:

https://bluecore.bcbst.com/caqh/Core

All payloads (X12 data) must be embedded using the Inline method (CDATA element) for real-time SOAP transactions.

4.4.2.5.2 Batch

Batch requests sent to the BlueCORE system must be submitted to the following URL:

https://bluecore.bcbst.com/caqh/Core

All batch payloads must be sent utilizing the SOAP Message Transmission Optimization Mechanism (MTOM) encapsulated MIME part. For more information, please see http://www.w3.org/TR/soap12-mtom/.

4.4.2.5.3 SOAP Header

The WS-Security Username and Password token (shown here with a gray background) is added to the SOAP Header by the platform on which SOAP is run. The SOAP platform's Web-Services Security Extensions may be configured to insert these tokens.

4.4.2.6 Examples

Below is an example of a SOAP request:

```
POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Type: application/soap+xml; charset=UTF-8; action="RealTimeTransaction"

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
      <soapenv:Header>
      <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
      secext-
      1.0.xsd" soapenv:mustUnderstand="true">
      <wsse:UsernameToken xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-
      wsswssecurity-
      utility-1.0.xsd wsu:Id="UsernameToken-21621663">
      <wsse:Username>bob</wsse:Username>
```

```
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
usernametoken-
profile-1.0#PasswordText">bobPW</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
    <soapenv:Body>
            <ns1:COREEnvelopeRealTimeRequest
            xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                   <PayloadType> X12_276_Request_005010X212</PayloadType>
                          <ProcessingMode>RealTime</ProcessingMode>
                          <PayloadID>f81d4fae-7dec-11d0-a765-
                          00a0c91e6bf6</PayloadID>
                          <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                          <SenderID>HospitalA</SenderID>
                          <ReceiverID>PayerB</ReceiverID>
                          <CORERuleVersion>2.2.0</CORERuleVersion>
      <Payload><![CDATA[ISA*00* *00* *ZZ*NEHEN780 *ZZ*NEHEN003
     ...IEA*1*000000031]]></Payload>
      </ns1:COREEnvelopeRealTimeRequest>
            </soapenv:Body>
</soapenv:Envelope>
```

Below is an example of a SOAP response:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml;
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransactionResponse";chars
et=UTF-8

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
      <soapenv:Body>
     <ns1:COREEnvelopeRealTimeResponse
     xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0xsd">
            <PayloadType>X12_277_Response_005010X212</PayloadType>
            <ProcessingMode>RealTime</ProcessingMode>
            <PayloadID>a81d44ae-7dec-11d0-a765-00a0c91e6ba0</PayloadID>
            <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
            <SenderID>PayerB</SenderID>
            <ReceiverID>HospitalA</ReceiverID>
            <CORERuleVersion>2.2.0</CORERuleVersion>
    <Payload><![CDATA[ISA*00* *00* *ZZ*NEHEN780 *ZZ*NEHEN003
     ...IEA*1*000000031]]></Payload>
            <ErrorCode>Success</ErrorCode>
            <ErrorMessage></ErrorMessage>
     </ns1:COREEnvelopeRealTimeResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

4.5 Username and Passwords

A unique user ID and password must be included when sending a transaction to the BlueCORE system. The method in which it is passed to the system for authentication is dependent upon the transaction type used; please refer to §4.4.1 - §4.4.2 for detailed information regarding supported transaction types.

4.5.1 BlueAccess

BlueCORE utilizes the authentication system built for BlueCross of Tennessee's online customer service portal called BlueAccess. Submitters obtain a user ID and password through registration at http://www.bcbst.com/blueaccess/. Registration instructions are shown below:

- Go to http://www.bcbst.com/blueaccess/.
- Select "Provider"
- Complete the registration form and click "Submit". The user ID, password and answer to token question are **case sensitive**. Please make note of the user ID and password. When submitting this user ID and password an exact match is required for successful authentication.

BlueAccess utilizes a "shared secret" process to control access to protected health information. In order to complete registration users of the BlueCORE system must associate at least **one** shared secret to their account. This shared secret is specific to providers contracted with BlueCross BlueShield of TN. Therefore, 3rd parties wishing to utilize the BlueCORE system **must** obtain the shared secret from one of their clients and add it to their account in order to successfully authenticate. The process for requesting a shared secret is shown below (please note however this request will go to the **provider** in question, regardless of the location of the requestor):

- Log back on to www.bcbst.com.
- On the BlueAccess section, type in your user ID and password.
- Scroll to the bottom of the page and click on the link for "Request Shared Secret."
- Submit the number(s) of BlueCross BlueShield of Tennessee provider(s) for which you are requesting a shared secret.
- A shared secret will be mailed **to the provider** within five business days for each provider number you entered.
- After you have obtained the shared secret from the provider, log back on to http://www.bcbst.com/.
- Key in your user ID and password on the BlueAccess portion of the home page.
- Scroll to the bottom of the page and click on the link for "Update Permissions."
- Click on the "Add Providers" button.
- Key in each provider number, federal tax id and shared secret.
- Click on "Submit" and the providers will be added.

5. CONTACT INFORMATION

5.1 EDI Customer Service & Technical Assistance

For questions regarding BlueCORE, ANSI, BlueAccess, or this guide, please contact:

BCBST e-Business Service Center
Monday – Friday, 8:00 AM – 6:30 PM Eastern
Ph: (423) 535-5717
Fax: (423) 535-1922

5.2 Provider Service Number

For questions regarding information related to subscribers (eligibility, claim status) that are non-technical, please contact

BCBST Provider Service
Monday – Friday, 8:00 AM – 5:15 PM Eastern
Ph: 1-800-924-7141

5.3 Applicable websites/email

EDI Customer Service & Technical Assistance

Email: Ecomm_techsupport@bcbst.com
Website: http://www.bcbst.com/providers/ecomm

Technical Support and Provider Service representatives are not available on scheduled company holidays.

For up-to-date information regarding BCBST's holiday schedules, please visit http://www.bcbst.com/contact-us/.

6. CONTROL SEGMENTS/ENVELOPES

6.1 ISA-IEA

The ISA segment terminator, which immediately follows the component element separator, must consist of only **one** character code. This same character code must be used as the segment terminator for each segment in the ISA-IEA segment set.

Files **must** contain a single ISA-IEA per transaction.

Incoming:

ISA01 – Authorization Information Qualifier – '00'
ISA02 – Authorization Information – always spaces
ISA03 – Security Information Qualifier – '00'
ISA04 – Security Information – always spaces
ISA05 – Interchange ID Qualifier (*Sender*) – 'ZZ'
ISA06 – Interchange Sender ID – "Tax ID"
ISA07 – Interchange ID Qualifier (*Receiver*) – 'ZZ'
ISA08 – Interchange Receiver ID – '00390'
ISA09 – Interchange Date – YYMMDD – provided by your software
ISA10 – Interchange Time – HHMM – provided by your software
ISA11 – Interchange Repetition Separator
ISA12 – Interchange Control Version Number – '00501'

ISA13 – Interchange Control Number – assigned by your software (usually sequential integer), no leading zeros allowed
ISA14 – Acknowledgement Requested – '1'
ISA15 – Usage Indicator – 'P' for Production, 'T' for Test
ISA16 – Component Element Separator (delimits components within a data element) provided by your software

IEA01 – Number of Included Functional Groups
IEA02 – Interchange Control Number – must match the Interchange Control Number in ISA13

Outgoing:

ISA01 – Authorization Information Qualifier – always '00'
ISA02 – Authorization Information – always spaces
ISA03 – Security Information Qualifier – always '00'
ISA04 – Security Information – always spaces
ISA05 – Interchange ID Qualifier (*Sender*) – 'ZZ'
ISA06 – Interchange Sender ID – '00390'
ISA07 – Interchange ID Qualifier -(*Receiver*)
ISA08 – Interchange Receiver ID –(Tax ID)
ISA09 – Interchange Date – YYMMDD – date processed
ISA10 – Interchange Time – HHMM – time processed
ISA11 – Interchange Repetition Separator
ISA12 – Interchange Control Version Number – '00501'
ISA13 – Interchange Control Number – Assigned by original sender's software
ISA14 – Acknowledgement Requested – '0' on 999 acknowledgements
ISA15 – Usage Indicator 'P' for Production, 'T' for Test
ISA16 – Component Element Separator – provided by your software

IEA01 – Number of Included Functional Groups
IEA02 – Interchange Control Number – must match the Interchange Control Number in ISA13

6.2 GS-GE

Files **must** contain a single GS-GE per batch or real time transaction

Incoming:

GS01 – Functional Identifier Code – 'HR' (for 276 transactions)
GS02 – Application Sender's Code – (Tax ID)
GS03 – Application Receiver's Code – '00390'
GS04 – Date – CCYYMMDD – provided by your software
GS05 – Time – HHMM – provided by your software
GS06 – Group Control Number – assigned by your software (usually sequential integer)

9 digit maximum, no leading zeros allowed
GS07 – Responsible Agency Code – ‘X’
GS08 – Version/Release/Industry Identifier Code – ‘005010X212’

GE01 – Number of Transaction Sets Included
GE02 – Group Control Number – must match Group Control Number in GS06

Outgoing:

GS01 – Functional Identifier Code – ‘HN’ (for 277 transactions)
GS02 – Application Sender’s Code – ‘00390’ (*Sender*)
GS03 – Application Receiver’s Code – (usually Tax ID)
GS04 – Date – CCYYMMDD – date processed
GS05 – Time – HHMM time processed
GS06 – Group Control Number – assigned number (usually sequential integer)
GS07 – Responsible Agency Code – ‘X’
GS08 – Version/Release/Industry Identifier Code – ‘005010X212’

GE01 – Number of Transaction Sets Included
GE02 – Group Control Number – matches Group Control Number in GS06

6.3 ST-SE

Each 276 request within a Batch transaction **must** be wrapped in its own ST-SE segment. Real-Time inquiries must contain only one ST-SE segment. Batch transactions are limited to 99 or less ST–SE groupings per batch file.

7. PAYER SPECIFIC BUSINESSS RULES AND LIMITATIONS

7.1 BCBST Specific Edits

BlueCORE currently responds with the following Claim Status Codes for common errors regarding claim information:

Problem	2200D / 2200E STC01-1	2200D / 2200E STC01-2
Claim Not Found	A4	35
Subscriber Not Found	E0	33
Patient Not Found	E0	97
Missing Information	E0	21

8. ACKNOWLEDGEMENTS

Real-time:

One of the following will be provided in response to a 276 inquiry:

- TA1 Interchange Acknowledgement if the ISA-IEA envelope cannot be processed.
- 999 Implementation Acknowledgement if the 276 transaction contains HIPAA compliancy errors within the ST-SE segments.
- 277 Response Transaction indicating the requested member's coverage or benefits.

Batch:

One of the following responses will be provided in response to a 276 inquiry:

- TA1 Interchange Acknowledgement available **within one hour** if the ISA-IEA envelope cannot be processed.
- 999 Implementation Acknowledgement (Reject) will be available **within one hour** if the 276 transaction contains HIPAA compliancy errors within the ST-SE segments.
- 999 Acceptance response will be available **within one hour**. The 277 transaction(s) will be available the following day (no later than 7:00a.m.) appended to the original 999 acceptance response.

9. TRADING PARTNER AGREEMENTS

A Trading Partner Agreement is not required for BlueCORE transactions. For information regarding registering as a user of the BlueCORE system, please see §4.5.

10. TRANSACTION SPECIFIC INFORMATION

Listed below are specific requirements that BlueCross BlueShield of Tennessee requires over and above the standard information in the ASC X12N 276/277 (005010X212) Health Care Claim Status Request and Response Implementation Guide.

We strongly recommend the use of upper-case alpha-characters. This will ensure data lookup compatibility.

Page #*	Loop ID	Reference	Name	Codes	Length	Notes/Comments
126	2100C	NM1	Provider Name			This is the provider filed on the claim in question
128	2100C	NM108	Identification Code Qualifier	XX		NPI required, therefore must use code 'XX'
128	2100C	NM109	Identification Code			Adjudicating provider NPI required
155	2200D	DTP	Claim Service Date			Subscriber DOS required if subscriber is patient
175	2100E	NM1	Dependent Name			Dependent name information
176	2100E	NM104	Name First			Dependent first name required
C.7		GS	Functional Group Header			Functional Group Information
C.8		GS06	Group Control Number			The Group Control Number may contain up to 9 characters, but it must not begin with a leading zero. For example 123456789 is valid, but 001234567 is not valid
C.9		GE	Functional Group Trailer			Functional Group Information
C.9		GE02	Group Control Number			The Group Control Number may contain up to 9 characters, but it must not begin with a leading zero. For example 123456789 is valid, but 001234567 is not valid

**ASC X12N 276/277 (005010X212) IG*, August 2006 edition*

A. APPENDICES

a. Implementation Checklist

BlueCross BlueShield of Tennessee suggests entities use the following information as a checklist of steps to become a BlueCORE submitter:

- Read and review this guide.
- Contact the e-Business Service Center (§5.1) with any questions regarding BlueCORE (if any).
- Register for a user ID (§4.5.1) for BlueAccess and complete the shared secret process.
- Send at least one test transaction (§2.3).
- Begin submitting BlueCORE transactions.

b. Business Scenarios

The following scenarios are intended to serve as examples of a typical relationship between entities and BlueCross BlueShield of Tennessee in regards to the BlueCORE system.

- *Clearinghouse A submits transactions for Provider A. Clearinghouse A wishes to provide real-time services for Provider A, so they register with their current payers to do real-time transactions via their respective implementations. In order to complete registration and successfully submit transactions on behalf of Provider A, Clearinghouse A must obtain a copy of the shared secret (§4.5.1) from Provider A to complete registration with BlueCross BlueShield of Tennessee. Once this has occurred, Clearinghouse A can send transactions for Provider A as well as any other clients it has a relationship with that are currently contracted with BlueCross BlueShield of TN.*

- *Software Vendor A provides practice management systems to Provider A. The system has the capability to build SOAP-based ANSI transactions for submission to various payers or clearinghouses. Provider A expresses an interest in being able to process real-time ANSI data so Software Vendor A instructs the provider on how to set up this feature. Provider A can then use their credentials they use for the BlueCross BlueShield of Tennessee BlueAccess system to send these transactions*

.

- *Provider A wishes to send real-time transactions, but does not have a clearinghouse relationship or practice management system that supports this feature. They therefore use in-house or contract talent to develop a customized HTTP MIME multipart submission page that they can then use in conjunction with their BlueAccess credentials to submit BlueCORE transactions.*

c. Frequently Asked Questions

Is there a charge for a provider to submit 276 requests and receive 277 responses back through the Blue CORE Web site?

This is a free service offered by BlueCross BlueShield of Tennessee to providers, clearinghouses and billing services and there are no fees associated with the use of this service.

Once a request is submitted when will a response be received back from BlueCross BlueShield of Tennessee?

A single real-time request will receive a response back within 20 seconds. A Batch request (multiple requests sent within one file) will receive a response back by 7 a.m. the next day.

Who do I call for support if a problem arises? What are the hours?

Contact:
e-Business Service Center at (423) 535-5717 or ecomm_techsupport@bcbst.com.
Monday through Friday from 8 a.m to 6:30 p.m.(ET).

I have successfully registered for a BlueAccess user ID and password, but I am receiving HTTP 401 errors when trying to submit a transaction.

Be sure you have completed the "shared secret" process as outlined in §4.5.1.