BCBST

ASC X12N 835 (005010X221A1) Health Care Claim Payment/Advice Standard Companion Guide

Refers to the Implementation Guides Based on ASC X12 version 005010

CORE v5010 Companion Guide

12/30/2013

Preface

This Companion Guide to the v5010 ASC X12N Implementation Guides and associated errata adopted under HIPAA clarifies and specifies the data content when exchanging electronically with BCBST. Transmissions based on this companion guide, used in tandem with the v5010 ASC X12N Implementation Guides, are compliant with both ASC X12 syntax and those guides. This Companion Guide is intended to convey information that is within the framework of the ASC X12N Implementation Guides adopted for use under HIPAA. The Companion Guide is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the Implementation Guides.

Table of Contents

1 INTRODUCTION

Under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Secretary of the Department of Health and Human Services (HHS) is directed to adopt standards to support the electronic exchange of administrative and financial health care transactions. The purpose of the Administrative Simplification portion of HIPAA is enable health information to be exchanged electronically and to adopt standards for those transactions.

1.1 SCOPE

This section specifies the appropriate and recommended use of the Companion Guide.

This companion guide is intended for BCBST Trading Partners interested in exchanging HIPAA compliant X12 transactions with BCBST. It is intended to be used in conjunction with X12N Implementation Guides and is not intended to contradict or exceed X12 standards. It is intended to be used to clarify the CORE rules. It contains information about specific BCBST requirements for processing following X12N Implementation Guides:

- 005010X221A1, Health Care Claim Payment/Advice (835)

All instructions in this document are written using information known at the time of publication and are subject to change.

1.2 OVERVIEW

This section specifies how to use the various sections of the document in combination with each other.

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 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, claim status, or claim remittance 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 any or all the CORE operating rules. Any entity that agrees to follow the CORE operating rules will be expected to exchange transactions per the requirements of the CORE rules and policies with all willing trading partners. Use of these rules by the industry will enhance the usability of transactions as well as decrease administrative costs and resources. See http://www.caqh.org/.

1.3 REFERENCES

1.3.1 ACS X12 Version 5010 TR3s: http://store.x12.org/store/healthcare-5010-consolidated-guides

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

1.3.3 CAQH/CORE: http://www.caqh.org/COREv5010.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

Definitions:

BlueCORE – This is BCBST's branded solution for provider and clearinghouse connectivity based on CORE standards, encompassing Phase I, II, and III capabilities.

Provider – Any healthcare provider rendering services to BCBST members.

Clearinghouse – Any 3rd party agent transacting data on behalf of a BCBST provider.

2 GETTING STARTED

2.1 WORKING WITH BCBST

Providers, and clearinghouses interested in requesting 835 transactions via BlueCross BlueShield of Tennessee's CORE Certified Solution, BlueCORE, should contact BlueCross BlueShield of Tennessee at (423) 535-5717, Monday through Thursday, 8 a.m. to 5:15 p.m. (ET), and Friday 9 a.m. to 5:15 p.m.

2.2 TRADING PARTNER REGISTRATION

Trading Partner Registration is required in order to receive 835 transactions via BlueCORE. Please visit http://www.bcbst.com/providers/ecomm/getting_started/index.shtml for additional information on becoming a BCBST trading partner.

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-coreera.bcbst.com/CAQHEraApp/batch

SOAP Request https://beta-coreera.bcbst.com/CAQHEraApp/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
    - https://beta-coreera.bcbst.com/CAQHEraApp/Core
- Retrieve appropriate response
- Review response to determine production readiness

4 CONNECTIVITY WITH THE PAYER/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 Batch

4.1.1.1 Submission

- The user application submits an HTTPS request to:
  - https://coreera.bcbst.com/CAQHEraApp/batch
- The user application submits a SOAP request to
  - https://coreera.bcbst.com/CAQHEraApp/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.
- BlueCORE then validates if the user submitting acknowledgement data is linked to the provider and/or clearinghouse records as a confirmed BCBST trading partner.
- 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.

4.1.1.2 Pickup

- The user submits an HTTPS / SOAP pick-up request* using the Payload ID to: https://coreera.bcbst.com/CAQHEraApp/batch
- 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.
- BlueCORE then validates if the user submitting acknowledgement data is linked to the provider and/or clearinghouse records as a confirmed BCBST trading partner.
- If the user is successfully authorized, all 835s available for the requested trading partner will be delivered.

4.2 TRANSMISSION ADMINISTRATIVE PROCEDURES

4.2.1 Structure Requirements

Batch 835 requests are limited to 1 pickup request per transaction.

4.3 RE-TRANSMISSION PROCEDURE

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 PROTOCOL SPECIFICATIONS

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:
        - Batch - for batch inquiries (either submission or pickup)
- Password (50 character max)
- PayloadType
    - Accepted values are:
        - X12_835_Request_005010X221A1
        - Batch Submission
        - X12_999_SubmissionRequest_005010X231A1
- PayloadID
    - Should conform to ISO UUID standards (described at http://www.rfc-editor.org/rfc/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address35, to ensure uniqueness.
- CORERuleVersion
    - Accepted value is:
        - 2.2.0
- SenderID (50 character max)
    - Must match 9 digit value in BCBST's trading partner database
- 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

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 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 Batch

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

https://coreera.bcbst.com/CAQHEraApp/batch

4.4.1.4 Examples

Below is an example of a HTTP MIME Multipart submission:

```
POST /core/eligibility 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_835_Request_005010X221A1
--XbCY
Content-Disposition: form-data; name=“ProcessingMode"
Batch
--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_835_Response_005010X221A1
--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 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

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 Batch

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

https://coreera.bcbst.com/CAQHEraApp/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/

4.4.2.5.2 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:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:cor="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soap:mustUnderstand="true">
<wsse:UsernameToken xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="UsernameToken-21621663">
  <wsse:Username>username</wsse:Username>
  <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-username-token-profile-
1.0#PasswordText">password</wsse:Password>
  </wsse:UsernameToken>
  </wsse:Security>
  </soap:Header>
<soap:Body>
<cor:COREEnvelopeBatchResultsRetrievalRequest>
  <PayloadType>X12_835_Request_005010X221A1</PayloadType>
  <ProcessingMode>BatchResultsRetrievalTransaction</ProcessingMode>
  <PayloadID>a3d3b8f340a511e3aa6e0804260c9a77</PayloadID>
  <PayloadLength />
  <TimeStamp>2013-12-10T14:57:00Z</TimeStamp>
  <SenderID>PayerA</SenderID>
  <ReceiverID>00390</ReceiverID>
```

```
  <CORERuleVersion>2.2.0</CORERuleVersion>
  <CheckSum>?</CheckSum>
  <Payload>cid:331143576196</Payload>
  </cor:COREEnvelopeBatchResultsRetrievalRequest>
  </soap:Body>
  </soap: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/RealTimeTransac
tionResponse";charset
=UTF-8
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-
envelope">
   <soapenv:Body>
      <ns2:COREEnvelopeBatchResultsRetrievalResponse
xmlns:ns2="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">

<PayloadType>X12_005010_Response_NoBatchResultsFile</PayloadType>

0<ProcessingMode>BatchResultsRetrievalTransaction</ProcessingMode>
         <PayloadID>a3d3b8f340a511e5aa6e1954770c9a78</PayloadID>
         <TimeStamp>2014-05-12T14:04:48-0400</TimeStamp>
         <SenderID>00390</SenderID>
         <ReceiverID>123456789</ReceiverID>
         <CORERuleVersion>2.2.0</CORERuleVersion>
         <CheckSum>?</CheckSum>
         <ErrorCode>Success</ErrorCode>
         <ErrorMessage>Request was processed
successfully</ErrorMessage>
      </ns2:COREEnvelopeBatchResultsRetrievalResponse>
   </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 – Thursday, 8:00 AM – 5:15 PM Eastern

Friday 9:00 AM – 5:15 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: eBusiness_Service@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:

ANSI 835 batch pickup requests do not contain inbound ISA data.

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

Incoming:

ANSI 835 batch pickup requests do not contain inbound GS data.

Outgoing:

GS01 – Functional Identifier Code – ‘HP’ (for 271 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 – “005010X221A1”

GE01 – Number of Transaction Sets Included

GE02 – Group Control Number – matches Group Control Number in GS06

6.3 ST-SE

Each 835 delivered as a result of a batch request may contain multiple ST/SE groupings per payment within a given ISA/IEA envelope.

7 PAYER SPECIFIC BUSINESS RULES AND LIMITATIONS

There are no specific rules and limitations for 835 pickup or acknowledgement submission for BCBST.

8 ACKNOWLEDGEMENTS AND/OR REPORTS

999 Functional Acknowledgements can be used to report errors or edits found during compliance check. See section 4.4.1.1 Header Requirements

9 TRADING PARTNER AGREEMENTS

9.1 TRADING PARTNERS

An EDI Trading Partner is defined as any BCBST customer (provider, billing service, software vendor, employer group, financial institution, etc.) that transmits to, or receives electronic data from BCBST.

Payers have EDI Trading Partner Agreements that accompany the standard implementation guide to ensure the integrity of the electronic transaction process. The Trading Partner Agreement is related to the electronic exchange of information, whether the agreement is an entity or a part of a larger agreement, between each party to the agreement.

For example, a Trading Partner Agreement may specify among other things, the roles and responsibilities of each party to the agreement in conducting standard transactions.

Trading Partner Registration is required in order to receive 835 transactions via BlueCORE. Please visit http://www.bcbst.com/providers/ecomm/getting_started/index.shtml for additional information on becoming a BCBST trading partner.

For information regarding registering as a user of the BlueCORE system, please see §4.5.

10 TRANSACTION SPECIFIC INFORMATION

This section describes how ASC X12N Implementation Guides (IGs) adopted under HIPAA will be detailed with the use of a table. The tables contain a row for each segment that BCBST has something additional, over and above, the information in the IGs. That information can:

1. Limit the repeat of loops, or segments

2. Limit the length of a simple data element

3. Specify a sub-set of the IGs internal code listings

4. Clarify the use of loops, segments, composite and simple data elements

5. Any other information tied directly to a loop, segment, composite or simple data element pertinent to trading electronically with BCBST

In addition to the row for each segment, one or more additional rows are used to describe BCBST's usage for composite and simple data elements and for any other information. Notes and comments should be placed at the deepest level of detail. For example, a note about a code value should be placed on a row specifically for that code value, not in a general note about the segment.

10.1 835 Health Care Claim Payment/Advice

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
69		BPR	Financial Information			
76		BPR16	Date			Dates within this segment will adhere to the following schedule: Wednesday - BCBST Facility Payments Thursday - BCBST Physician Payments If a payment date falls on a recognized bank holiday, then the date will move to the previous business day.

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 financial services for Provider A, so they register with their current payers to do 835 transactions via their respective implementations. In order to complete registration and successfully retrieve transactions on behalf of Provider A, Clearinghouse A must obtain a copy of the shared secret (§4.5.1) from Provider A and register as a valid trading partner 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 ANSI 835 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 retrieve these transactions as long as their Trading Partner agreement includes 835 transactions.
- Provider A wishes to retrieve 835 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 request page that they can then use in conjunction with their BlueAccess credentials to retrieve transactions as long as their Trading Partner agreement includes 835 transactions.

c. Frequently Asked Questions

Is there a charge for a provider to receive 835 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 batch 835 request will receive a response back within the same session, but response times may vary depending on the size of the 835 payload being delivered and internet speeds. A Batch request (multiple requests sent within one file) will receive a response back by 7a.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

Monday – Thursday, 8:00 AM – 5:15 PM Eastern

Friday 9:00 AM – 5:15 PM Eastern or

eBusiness_Service@bcbst.com

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.