blue 🛡 of california

278-13/278-11 HIPAA Transaction Companion Guide

HIPAA/V5010X217

Version: 1.2

9/11/2018

Document History

DOCUMENT VERSION HISTORY TABLE

Version	Sections Revised	Description	Revised By	Date
1.0		Initial	Paula Arenz	6/1/2014
1.1	Appendix Trading Partner Agreement	Updated Trading Partner Agreement	Chris Hoover	9/5/2018
1.2	5 Contact Information	Added EDI Inquiry tool link	Bishal Malla	9/11/2018

Table of Contents

1 Introduction

This Companion Guide to the v5010 ASC X12N 278-13 and 278-11 Implementation Guides and associated errata adopted under HIPAA, clarifies and specifies the data content when exchanging eligibility data electronically with Blue Shield of California (BSC) Health Plan. 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.

1.1 Scope

This document should be used as a guide when sending or receiving authorization or certifications data via a standard 278-13/278-11 EDI transaction to the BSC EDI system.

BSC EDI is a system through which trading partners can submit 278-13 EDI transactions as well as receive 278-11 EDI transactions. This document describes how a submitter uses the system to submit files and receive acknowledgements and reports.

Before using BSC EDI Channel, it is important to determine your compatibility in relation to BSC EDI Channel.

1. You must be able to send and receive X12 health care EDI files.

2. You must be able to extract information from your system and interpret it.

3. You must have sufficient EDI technical knowledge to make adjustments to your system, as necessary.

4. You must be able to interact with BSC EDI Channel.

5. Overview

This companion document has been separated into multiple sections:

1. Getting Started

2. Connectivity with Payer/Communications

3. Contact Information

4. Control Segments/Envelopes

1.2 References

The standard HIPAA transaction implementation guides are referenced by this guide. Copies of current guides may be obtained from www.wpc-edi.com

1.3 Additional Information

This document was developed to provide users of BSC EDI with the necessary information in order to exchange EDI transactions with BSC. With the assumption that the user has working level EDI knowledge, this document focuses on the use of the BSC EDI system and does provide background information on EDI transactions and their use.

2 Getting Started

2.1 Working with Blue Shield of California

This guide includes the instructions you will need to get connected and start sending/receiving standard 278-13 and 278-11 transactions with BSC. Make sure you read the entire guide in order to take advantage of the full functionality of the system.

2.2 Trading Partner Registration

Before submitting or receiving a 278-13 or 278-11 transaction, you must register as a Trading Partner with BSC to ensure you are established and recognized in our system. To register, please fill out the Enrollment Application and Trading Partner Agreements and submit to:

Email: edi_bsc@blueshieldca.com
Fax: 530-351-6150

2.3 Certification and Testing Overview

The purpose of BSC EDI testing phase is to provide you with a mechanism to produce the same reports and acknowledgments that are produced once you are in production. This allows you to test your ability to produce correct data content and to receive and process the acknowledgments and files we produce for you. By testing with BSC EDI, you will be allowed to send transactions. Transactions go from you to BSC Non-Production Environment, as would be the case in a Production Environment.   A general breakdown of the process goes like this:

1. You will be set up with connectivity to perform connectivity testing.

2. You would receive one of 3 acknowledgments: a 278-11 response, a TA1 acknowledgment, or a 999 rejection.

3. The 999 will show any errors or problems that were found in the transaction sent. The errors or problems could be related to the HIPAA standards or directly to the BSC Companion Guide.

4. You will continue to test until you have resolved any issues. Then, request to have your status for the specific transaction you have been testing changed from test to production.

5. Your test to production status change request will be reviewed by BSC and you will be notified via email when your request has been approved.   When your request has been approved you will be notified that you are now able to send transactions in Production.

More than one transaction type can be run simultaneously. You can also be granted production status for one type of transaction and still be in test mode for other transactions.

There are no technical limits to the number of transactions you can submit in a single batch file; however, there are some practical limits. Files with large numbers of transactions will generate reports with large amounts of data. Keep this in mind as you prepare your systems to send files to BSC EDI. For Real-Time transactions you will need to send one 278-13 transaction request per file.

The communication protocol is tested as a part of first-time testing. Any time a communication protocol is changed, some testing is needed. The communication protocols for sending transactions to BSC EDI are the same for testing as for production.

3 Testing With Payer

After we receive and process your EDI Registration Form, your BSC EDI Analyst will work with you through our testing process. Our testing process is required for all trading partners in order to minimize production problems.

If you have questions or concerns about testing, please call our EDI Analyst. See Section 5 for contact information.

Proper preparation before testing will ease the testing process and promote its success.

Trading Partners must:

- Read and make sure that you understand the terms and conditions of the BSC Trading Partner Agreement (TPA), accept the conditions and terms of the TPA.

- Read all chapters and appendices of this Companion Guide.

- Complete and email, fax or mail the BSC Registration Form with the required attachments to your BSC EDI Analyst.

- After we receive and process you completed EDI Registration Form, your BSC EDI Analyst will contact you to discuss your testing schedule and the testing process.

3.1 Testing and Production Phases

 You will need to repeat the following Phase I and Phase II testing procedures for each transaction type that you want to submit.

Phase I: Testing EDI Connections in Non-Production Environment (Using Limited Test Data)

The BSC Trading Partner X12 testing process has 2 phases as well for the 278-13.

1. Checks the outer envelope in the order of the transaction segments

2. Checks values to ensure that they comply with the specifications in the X12 Implementation Guides. During this 2nd section, you will submit test files and receive acknowledgments in response to your files.

Upon Receipt of your BSC Trading Partner Registration form and the required attachments, your BSC EDI Analyst will contact you to schedule Phase I testing.

Creating and Submitting Your Test Files

Please ensure that your Phase I test files abide by the following instructions:

- Create test files with X12 version 005010.

- Limited set of agreed upon test scenarios.

- Create test files using the same means you will use to create files for productions data. The test files must contain realistic data. Do not handcraft data specifically for testing.

- Include a representative sampling of the types of transactions you typically submit.

- In the Interchange Control Header, ISA15 (Usage Indicator), enter T to indicate test data.

Upon successful completion of Phase I, Phase II can begin. Phase II checks values to ensure that they comply with the specification in the X12 Implementation Guides. During Phase II, you will submit test files and receive reports in response to your files. To test 27X files, you will construct and submit test files as explained in this section.

Phase II: Production (validation testing) to make sure TP setup has been promoted to Production environment.

Once you have received production status for a transaction, BSC recommends that you send a limited run of production data. This will help ensure that it will be easier to troubleshoot problems that may arise during the first few production runs. It is up to you how many transactions you send, but you should use prudence as you select the size and scope of the first few production runs.
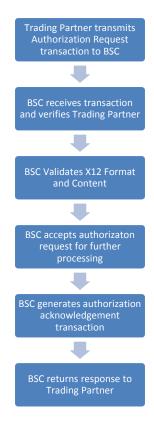
Once out of testing mode, you will send real transactions that will be processed by BSC production applications. You will receive reports related to your production file submissions and the actual X12 transactions generated by BSC production applications in response to your production file submissions.

Note: Ensure that your ISA15 is set to "P" when submitting transactions for Production.

4 Connectivity with the Payer/Communications

4.1 Process Flows

The following is a high level process flow of a 278-13/278-11 Transaction

```
┌─────────────────────────┐
│  Trading Partner transmits │
│  Authorization Request     │
│  transaction to BSC        │
└─────────────────────────┘
            ↓
┌─────────────────────────┐
│  BSC receives transaction  │
│  and verifies Trading Partner │
└─────────────────────────┘
            ↓
┌─────────────────────────┐
│  BSC Validates X12 Format  │
│  and Content               │
└─────────────────────────┘
            ↓
┌─────────────────────────┐
│  BSC accepts authorizaton  │
│  request for further       │
│  processing                │
└─────────────────────────┘
            ↓
┌─────────────────────────┐
│  BSC generates authorization │
│  acknowledgement           │
│  transaction               │
└─────────────────────────┘
            ↓
┌─────────────────────────┐
│  BSC returns response to   │
│  Trading Partner           │
└─────────────────────────┘
```

4.2 Transmission Administrative Procedures

Schedule, Availability, and Downtime Notification

Effective January 2013, the BSC 278-13/278-11 system is available:

Real Time: Sunday 22:00 through Saturday 21:59 PST
Batch Transactions: 24x7 Sunday through Saturday

BSC will notify Trading Partners of any additional planned downtime via e-mail.

Any unplanned downtime will be communicated to Trading Partners via e-mail. A follow up e-mail will be sent once the system becomes available.

4.3 Re-Transmission Procedure

Trading Partners may contact BSC for assistance in researching problems with their transactions. However, BSC will not edit Trading Partner authorization data and/or resubmit transactions for processing on behalf of a Trading Partner. The transaction must be corrected and re-submitted by the Trading Partner.

4.4 Communication Protocol Specifications

BSC receives and transmits transactions using MQ and HTTP/s protocols for real-time mode, and sFTP and HTTP/s for batch mode.

For MQ, both server-to-server and client-to-server connections are supported. B2B VPN connectivity must be established between both the Trading Partner and BSC. Separate MQ connections must be made for each inquiry transaction type, however a single MQ connection may be used for the receipt of all registered transaction responses from BSC.

BSC supports CORE Phase II HTTP/s open connectivity standards, HTTP MIME Multipart and SOAP+WSDL, for both real-time and batch modes.

Specific connectivity information, including passwords, will be provided to you once you send in your Trading Partner Registration.

Unique file naming conventions are required for batch mode transactions:

1.) A standard naming convention is required to be used for the files you will be sending to BSC. The file convention is stated as the following:
SubmitterID_Date_Time.278

i.e.: **Submitter ID_YYYYMMDD_HHMMSS.278**

2.) The outbound file naming convention for 278-11 files in response to 278-13 files shall be as follows:
[InterchangeRecieverID]_HHmmsssSSSSyyyyMMddX217.278 Where HHmmsssSSSSyyyyMMdd is two digit hour, two digit minutes, seconds with leading zeros, milliseconds with leading zero, four digit year, two digit month and two digit day followed by value "X217" to identify 278-11 files in response to a 278-13 request.
Example: 12345_1600001043220140713X217.278

5 Contact Information

For support and questions with EDI transactions, you can submit your request with Personal Health Information (PHI) securely online using our EDI Inquiry tool on Provider Connection.

https://www.blueshieldca.com/provider/claims/electronic-transactions/submit-edi-inquiry.sp

EDI Customer Service: 1-800-480-1221

EDI Technical Assistance: 1-877-747-6800

Provider Service Number: www.blueshieldca.com/provider   Phone#: 1-800-258-3091 Opt #3 for provider contract related questions.

Applicable Websites/E-Mail:

www.blueshieldca.com/provider

EDI_BSC@blueshieldca.com

www.blueshieldca.com

6   Control Segments/Envelopes:

6.1   ISA-IEA Envelope Data

BSC uses the v5010 ASC X12N 278 Implementation Guide and associated errata adopted under HIPAA. This specifies the data content for the 278 transaction data that you will be getting from the Blue Shield of California (BSC) Health Plan. BSC has not made any changes or customizations to this format. You may purchase a copy of the 278 implementation guide from the Washington Publishing Company at http://www.wpc-edi.com.

The Interchange Control Header (ISA) is the first record of the entire Interchange. Every X12 Interchange must begin with an ISA Segment.

Purpose: To start and identify an interchange of zero or more functional groups and Interchange-related control segments.

File Delimiters:

1. **ISA Segment**: This segment is 106 byte fixed length record. Insert trailing spaces after String type (AN) element values and leading zeroes before Numeric type (Nn) element values as needed to comply with the length requirement.

2. **Data Element Separator**: The fourth byte within the ISA record (the first byte after ISA) tells the receiver what value the sender is using as a data element separator. The value used as the data element separator must not be present within any data element in the transaction.

   a. To BSC: Send the value used as the Data Element Separator in the transaction following this ISA segment.

   b. From BSC: In response to the 278-13 transactions, the value sent to BSC with ISA record accompanying the 278-13 will be returned on the 278-11 response.

3. **Repetition Separator**: Byte 83 (ISA11) within the ISA record is a simple or composite data elements within a segment that can be designated as repeating data elements. Repeating data elements are adjacent data elements that occur up to a number of times specified in the standard as number of repeats.

   a. To BSC: Send the value used as the Repetition Separator in ISA11 of the transaction.

b. From BSC: In response to the 278-13 transactions, the value sent to BSC with ISA record accompanying the 278-13 will be returned on the 278-11 response.

4. **Component Element Separator**: Byte 105 (ISA16) within the ISA record. This delimiter is used to separate Composite Data Structure which is an intermediate unit of information in a segment. Composite Data Structures are composed of one or more logically related simple data elements, each, except the last, followed by a Component Element Separator.

   a. To BSC: Send the value used as the Component Element Separator in ISA16 of the transaction.

   b. From BSC: In response to the 278-13 transactions, the value sent to BSC with ISA record accompanying the 278-13 will be returned on the 278-11 response.

5. **Segment Terminator**: Byte 106 within the ISA record. The data segment is a unit of information in a transaction set. A data segment consists of a segment identifier, one or more composite data structures or simple data elements each proceeded by a data element separator and succeeded by a segment terminator.

   a. To BSC: Send the value used as Segment Terminator in byte 106 within the ISA record of the transaction.

   b. From BSC: In response to the 278-13 transactions, the value sent to BSC with ISA record accompanying the 278-13 will be returned on the 278-11 response.

Example: ISA✲ 00✲ ....✲ 01✲ SECRET....✲ ZZ✲ SUBMITTERS.ID..✲ ZZ✲ RECEIVERS.ID...✲ 930602✲ 1253✲ }✲ 00501✲ 000000905✲ 1✲ T✲ :~

Table:

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
ISA01	Authorization Information Qualifier	M	ID	(2/2)	00=No authorization info present. 03=Additional data identification	0
ISA02	Authorization Information	M	AN	(10/10)	If ISA01=00, must be 10 spaces. If ISA01=03, must be mutually agreed upon.	10 spaces
ISA03	Security Information Qualifier	M	ID	(2/2)	00=No security info present. 01=Password.	0
ISA04	Security Information	M	AN	(10/10)	IF ISA03=00, must be 10 spaces. IF ISA03-01, must be mutually agreed upon.	10 spaces

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
ISA05	Interchange Sender ID Qualifier	M	ID	(2/2)	01=Duns 14=Duns plus suffix 20=Health insurance number (HIN) 27=CMS carrier ID number 28=CMS fiscal intermediary ID number 29=CMS Medicare provider /supplier ID 30 U.S. federal tax ID 33=NAIC ID ZZ=Mutually defined.	To BSC: Use the value that best describes the sender ID in ISA06. If the value in ISA06 is an ID assigned to the sender by BSC or Enumeron LLC, use ZZ. From BSC: ZZ
ISA06	Interchange Sender ID	M	AN	(15/15)		To BSC: Send the value entered as your sender ID on the Registration or Settings page, left justified. From BSC: 940360524, left justified.
ISA07	Interchange Receiver ID Qualifier	M	ID	(2/2)	See ISA05 for values	To BSC: ZZ From BSC: In response to 278-13 transactions, the value sent to BSC in the ISA05. In other transactions BSC will send ZZ.
ISA08	Interchange Receiver ID	M	AN	(15/15)		To BSC: 940360524, left justified. From BSC: in responses to 278-13 transactions, the value sent to BSC in the ISA06.
ISA09	Interchange Date	M	DT	(6/6)	Format=YYMMDD	Date from sending system.
ISA10	Interchange Time	M	TM	(4/4)	Format=HHMM	Time from sending system using 24 hour format. E.G., for 1 PM use 1300. From BSC: this will be EST.

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
ISA11	Repetition Separator	M	ID	(1/1)		{
ISA12	Interchange Control Version Number	M	ID	(5/5)	00501	00501
ISA13	Interchange Control Number	M	N0	(9/9)	Must be the same as the value sent in the following IEA02	To BSC: Must be a unique sequential number that does not repeat within a 180-day period. From BSC: In responses to 278-13 transactions, the value sent to BSC in the ISA13. Otherwise, an BSC assigned unique sequential number that does not repeat within a 180-day period.
ISA14	Interchange Acknowledgment Accepted	M	ID	(1/1)	0=No interchange ACK requested. 1=Interchange ACK requested	To BSC: in 278-13 transactions: Must be 0.
ISA15	Usage Indicator	M	ID	(1/1)	T=Test P=Production	T=Test P=Production
ISA16	Component Element Separator (also referred to as "sub-element separator"	M	n/a	(1/1)	The value used as Component Element Separator must no be present for any other reason within any data element in the transaction.	To BSC: The value that is used as the component element separator in the transaction following this ISA segment. From BSC: In responses to 278-13 transactions, the value sent to BSC is the ISA16.

There are several things you can use for the sender ID, as outlined in the HIPAA Implementation Guides. A summary of those guidelines is included here for your perusal.

The qualifier that designates the type of the sender ID is sent in the ISA05 and can be one of the following:

01=Duns (Dun & Bradstreet)

14=Duns plus suffix

20=Health Industry Number (HIN)

17=Carrier Identification Number as assigned by CMS

29=Fiscal Intermediary Number as assigned by CMS

30=US Federal Tax ID

13

33=NAIC Code

ZZ=Mutually Defined

IEA-Interchange Control Trailer

The Interchange Control Trailer (IEA) is the last record of the entire Interchange. Every X12 Interchange must end with an IEA segment.

Example: IEA*1*000000905~

Purpose: To define the end of the interchange of zero or more functional groups and interchange-related control segments.

Table:

Seg/Fld	Name	Req	Type	Min/Max	Values allowed by X12 Standards	Values to be used with BSC
IEA01	Number of Functional Groups	M	N0	(1/5)	The total number of functional groups (GS-GE) contained in the interchange (ISA-IEA)	As required by standard.
IEA02	Interchange Control Number	M	N0	(9/9)	Must be the same as the value sent in the proceeding ISA13.	As required by standard.

6.2 GS-GE-Functional Group Header

The Functional Group Header (GS) is the first record of an entire Functional Group. Every X12 Functional Group must begin with a GS segment.

GS Example: GS*HS*SENDER CODE*RECEIVER CODE*19971001*0802*1*X*005010X217~

GS Purpose: To indicate the beginning of the functional group and to provide control information.

Table

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
GS01	Functional ID Code	M	ID	(2/2)	FA=999 - Functional ACK HI=278-13 Authorization.	Must reflect the transaction being submitted within the Functional Group.

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
GS02	Application Sender's Code	M	AN	(2/15)		To BSC: Send the value entered as your Submitter Id on the Registration or Settings page, left justified. From BSC: In responses to 278-13 transactions, the value sent to BSC in the GS03. Otherwise, the value entered as your Submitter Id on the Registration or Settings page.
GS03	Application Receiver's Code	M	AN	(2/15)		To BSC: Must reflect the transaction being submitted within the Functional Group using the values listed below. **Eligibility: 278-13 is 940360524.** All other transactions: Send the value 940360524 (the value also sent in the ISA08, without trailing spaces).
GS04	Date	M	DT	(8/8)	Format=CCYYMMDD	Date from sending system.
GS05	Time	M	TM	(4/8)	Format=HHMM	Time from sending system using 24 hour format; e.g., for 1 PM, use 1300. From BSC, this will be EST.
GS06	Group Control Number	M	N0	(1/9)	Must be equal to the value sent in the following GE02	A number assigned by the sender that is unique to each functional group within this interchange.
GS07	Responsible Agency Code	M	ID	(1/2)	X=ASC X12	X
GS08	Version/Release/Industry ID Code	M	AN	(1/12)	005010=999 00501X217=278-13/278-11	Must reflect the transaction being submitted within the Functional Group using the values listed to the left.

GE-Functional Group Trailer

The Functional Group Trailer (GE) is the last record of an entire Functional Group. Every X12 Functional Group must end with a GE Segment.

Example: GE*1*1~

Purpose: To indicate the end of a functional group and to provide control information.

Table:

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
GE01	Number of Transaction Sets Included	M	N0	(1/6)	The total number of transaction sets (ST-SE) contained in the Functional Group (GS-GE)	As required by standard
GE02	Group Control Number	M	N0	(9/9)	Must be the same as the value sent in the preceding GS06.	As required by standard

6.3 ST-SE Transaction Set Header

The Transaction Set Header (ST) is the first record of an entire Transaction Set. Every X12 Transaction set must begin with an ST Segment.

Example: ST*999*1234~

Purpose: To indicate the start of a transaction set and assign a control number.

Set Notes:

1.   These acknowledgments shall not be acknowledged, thereby preventing an endless cycle of acknowledgments. Nor shall a Functional Acknowledgment be sent to report errors in a previous Functional Acknowledgment.

2. The Functional Group Header Segment (GS) is used to start the envelope for the Functional Acknowledgment Transaction Sets. In preparing the functional group of acknowledgments, the application senders code and the application receiver's code, take from the functional group being acknowledged, are exchanged; therefore, one acknowledgment functional group responds to only those functional groups from one application receivers code to one application senders code.

3. There is only one Functional Acknowledgment Transaction Set per acknowledged functional group.

Table

Seg Fld	Name	Req	Type	Min Max	Values allowed by X12 Standards	Values to be used with BSC
ST01	Transaction Set ID Code	M	ID	(3/3)	999: Functional Acknowledgment 278-13: Authorization Review Request 278-11: Authorization Review Response/Information	As required by standard

					Must be the same as the value sent in the following SE02	As required by standard
ST01	Transaction Set Control Number	M	AN	(4/9)		

SE-Transaction Set Trailer: The Transaction Set Trailer (SE) is the last record of an entire Transaction Set. Every X12 Transaction Set must end with an SE Segment.

Purpose: To indicate the end of the transaction set and provide the count of the transmitted segments (including the beginning (ST) and ending (SE) segments).

Example: SE*27*1234~

Table:

Seg/Fld	Name	Req	Type	Min/Max	Values allowed by X12 Standards	Values to be used with BSC
SE01	Number of Segments Included	M	N0	(1/10)	The total number of segments contained in the transaction set (ST-SE), including the ST and SE segments.	As required by standard
SE02	Transaction Set Control Number	M	AN	(4/9)	Must be the same as the value sent in the preceding ST02	As required by standard

7 Payer Specific Business Rules and Limitations

The purpose of this section is to delineate specific data requirements as they apply to 278-13/278-11 authorization review request. BSC supports processing 278-13 authorization or certification request and will respond with a 278-11 acknowledging receipt containing a closed pended status (BHT06=18 and HCR01=A4). Any further status updates are provided outside of the 278 transactions via Blue Shield of CA Provider Website (www.blueshieldca.com/provider) or Provider Customer Service (see section 5 for contact information).

8 Acknowledgments and Reports-Reports Inventory

The purpose of this section is to outline the BSC processes for handling the initial processing of incoming files and electronic acknowledgments.

TA1 Interchange Acknowledgment Transaction

All X12 file submissions are pre-screened upon receipt to determine if the interchange control header (ISA) or interchange control trailer (IEA) segments are readable. If errors are found, a TA1 response transaction will be sent to notify the trading partner that the file could not be processed. No TA1 response transaction will be sent for error-free files.

999 Functional Acknowledgment Transaction

If the file submission passes the ISA/IEA pre-screening above, it is then checked for ASCX12 syntax and HIPAA compliance errors. When the compliance check is completed, a 999 will be sent to the trading partner informing them if the file has been accepted or rejected. If multiple transaction sets (ST-SE) are sent within the functional group (GS-GE, the entire functional group (GS-GE) will be rejected when an ASCX12 or HIPPA compliance error is found.

9 Trading Partner Agreements

Please reference Section 11-Appendices: Trading Partner Agreement.

10 Transaction Specific Information

Please reference Section 11-Appendices: BSC 278-13/278-11 Companion Guides (BSC-278-13-5010 CG/BSC-278-11-5010-CG).

11 Appendices

Additional Attachments:

- BS Trading Partner Agreement

- BSC EDI Enrollment Form
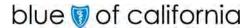
- BSC Connectivity Detail Form

Blue Shield of California
Electronic Data Exchange
Trading Partner Agreement

This Trading Partner Agreement ("Agreement") is made as of _____, between California Physicians' Service dba Blue Shield of California, for and on behalf of itself and its Affiliates and subsidiaries, including Blue Shield of California Life & Health Insurance Company and Care 1st Health Plan (collectively "Blue Shield") and

_____ ("Trading Partner").

Trading Partner Name (please print)

A. Conducting Transactions

1. The parties shall exchange electronic transactions, which may include claim submissions, eligibility requests, claims status, authorizations, remittance advice, and/or electronic funds transfer. Trading Partner shall conform transactions to the applicable Blue Shield Companion Guide. Blue Shield may modify its Companion Guides at any time without amending this Agreement.

2. Blue Shield may reject any transaction that does not conform to the applicable transaction Companion Guide and HIPAA compliance edits.

3. Trading Partner and Blue Shield shall cooperate in testing the exchange of transactions, as Blue Shield deems appropriate. Testing will be designed to ensure the accuracy, timeliness, completeness, and security of each data transmission.

4. Each party shall take reasonable care to ensure information in each electronic transaction is timely, complete, accurate, and secure.

5. A party that receives from the other party a transaction not intended for the recipient shall immediately notify the other party to arrange for the return or destruction of the transaction, as the other party directs. A party that has evidence of a lost or indecipherable data transaction from or to the other party, shall immediately notify the other party to arrange for retransmission of the transaction.

6. Each party is responsible for all costs, charges, or fees it may incur by transmitting electronic transactions to, or receiving electronic transactions from, the other party.

7. Blue Shield will not send Trading Partner a health care provider's electronic remittance advice (ERA-835) unless (a) Trading Partner is the health care provider or (b) Trading Partner is named in a "Provider Authorization Form" as an authorized recipient of the health care provider's electronic remittance advice.

8. Blue Shield will only make electronic funds transfers to an authorized financial institution.

B. Privacy and Security

1. Each party is responsible for the accuracy, privacy, and security of transactions it submits to the other party, in accordance with state and federal laws, including the Administrative Simplification requirements of HIPAA, as set out in the Code of Federal Regulations Title 45 Parts 160164. Each party is solely responsible for the preservation, privacy, and security of data in its possession and during transmission, until the data are received by the other party.

2. Each party shall implement reasonable and appropriate safeguards to prevent unauthorized access to (a) its own and the other party's transmission and processing systems, (b) transactions with the other party, and (c) the control structure applied to transmissions between the parties. Such safeguards will include steps to prevent persons with authorized access from exceeding the scope of their access.

3. Each party shall implement reasonable and appropriate safeguards designed to prevent any person from circumventing security mechanisms or procedures safeguarding its own or the other party's computer systems or data.

4. Trading Partner shall treat and shall require its employees and agents to treat any user ID or password confidentially.

C. General Terms

1. Trading Partner agrees to require its employees and agents to comply with the terms of this Agreement.

2. This Agreement is effective when Blue Shield receives a copy of the Agreement signed by Trading Partner.

3. Each party shall establish and maintain a "Trade Data Log," in which the parties shall record all transactions exchanged with the other party under this Agreement. Each party shall take reasonable steps to ensure that the

Trade Data Log is a current, accurate, complete, and unaltered record of all data transmissions between the parties. Each party shall maintain accurate, complete, and unaltered copies of the Trade Data Log for ten (10) years. This paragraph shall survive the termination of the Agreement for any reason.

4. Trading Partner shall allow and shall require its agents to allow Blue Shield to audit Trading Partner's and Trading Partner's agents' Trade Data Log, operating systems, and relevant business records to assess Trading Partner's compliance with this Agreement. Blue Shield's audit may evaluate security precautions implemented by Trading Partner and Trading Partner's agents. Trading Partner shall cooperate and shall require the cooperation of its agents with any audit related to this Agreement by a governmental agency, licensing body, or accreditation body.

5. Should one party materially breach this Agreement, the other party may give the breaching party written notice of the breach and the breaching party shall have thirty (30) days to cure the breach. If the breaching party does not cure the breach within the thirty (30) day period, the nonbreaching party may, in its sole discretion, either extend the cure period or give a written termination notice that becomes effective five (5) working days thereafter.

The parties acknowledge, agree to and shall be bound by all of the terms, provisions and conditions of the Agreement with the execution hereof by duly authorized representatives:

TRADING PARTNER		CALIFORNIA PHYSICIANS' SERVICE dba BLUE SHIELD OF CALIFORNIA
		By: _____
By: _____ _____		
Title: _____ _____		Title: Manager, EDI Platform Services
Date: _____ _____		Date: _____
TIN:_____ _____		
Telephone: _____		Telephone: 800-480-1221
Fax: _____ _____		Fax: 530-351-6150
E-Mail:_____ _____		E-mail: edi_bsc@blueshieldca.com

blue of california

Trading Partner Enrollment Form

☐ **Trading Partner will exchange transactions directly with Blue Shield of California using sFTP or Http/s**

Transactions Elected:	☐ 837 Claims/Encounter Submission ☐ 276/277Claims Status ☐ 270/271 Eligibility
	☐ 835 ERA/EFT ☐ 278 Authorizations

Blue Shield of California providers must use the Provider Authorization Form to enroll in electronic remittance advice and provide bank routing information for electronic funds transfer (EFT). Additional copies of this form are available online at blueshieldca.com/provider/edi.

During exchange of electronic transactions, each party will comply with all applicable requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated thereunder.

For Claim 837 enrollment, clearinghouses representing multiple providers or providers with multiple Tax Identification Numbers (TINS) or Type II NPI(s) must use the Tax Identification Detail form to indicate all Tax Identification numbers for which data will be included in EDI transmissions.

Business Type:	☐ Clearinghouse ☐ Billing Service ☐ Vendor ☐ MSO/CBO
	☐ Institutional provider ☐ Professional provider ☐ IPA

Trading partner name:			
Tax ID:	National Provider Identifier (NPI) Type 2:		
Street Address:			
City:		State:	Zip:
Mailing address:			
City:		State:	Zip:
Contact name:	Phone:		Fax:
Contact title:	Email:		

Software Vendor Information (if applicable)

Software vendor contact name:
Vendor address

Blue Shield of California
Attn: EDI
4700 Bechelli Lane
Redding, CA 96002

Fax to: EDI/Blue Shield at (530) 351-6150
Email: EDI_BSC@blueshieldca.com

Trading Partner Enrollment Form

An Independent Member of the Blue Shield Association

blue of california

Blue Shield of California
Attn: EDI
4700 Bechelli Lane
Redding, CA 96002

Fax to: EDI/Blue Shield at (530) 351-6150
Email: EDI_BSC@blueshieldca.com

Trading Partner Enrollment Form

blue of california

Connectivity Detail Form

Complete this form to establish a direct connection with Blue Shield.

Contact Information *(at least two contacts are required):*			
Contact Type	**Name**	**Phone**	**Email**
Business			
Technical Lead			
Primary User			
Backup User			

COMPLETE INFORMATION BELOW FOR SECURE FILE TRANSFER PROTOCOL (sFTP)

Data Integrity Protocol (select one):

Not Required ☐	SHA-1 ☐	MD5 ☐	RIPEMD-160 ☐

Transport Method & Data Encryption (select one):

Secure FTP over SSH with no PGP data encryption ☐	Secure FTP over SSH with PGP encryption of data ☐

PGP Encryption Method (please select only one):

AES (128 bit)☐	Diffie-Hellman (1024 bit)☐	RSA (1024 bit) ☐
AES (192 bit)☐	Diffie-Hellman (2048 bit)☐	RSA (2048 bit) ☐
AES (256 bit)☐	Diffie-Hellman (4096 bit)☐	RSA (4096 bit)☐
Cast 5 (128 bit)☐	El Gamal (1024 bit)☐	Triple DES (168 bit) ☐
DSA v3 & v4 (1024 bit)☐	El Gamal (2048 bit)☐	Two Fish (256 bit) ☐
DSA v3 & v4 (2048 bit)☐	El Gamal (4096 bit) ☐	
DSA v3 & v4 (4096 bit) ☐	IDEA (128 bit) ☐	

Static DNS Name and/or Static IP Address & Data Delivery Method (select one):

Primary DNS Name and/or IP address**: (   ).(   ).(   ).(   )**

Secondary DNS Name and/or IP address: (   ).(   ).(   ).(   )

IP addresses must be static. For IP address not registered in the name of the trading partner, complete the IP Ownership Verification Form.

NOTE: Notify Blue Shield of California at (800) 480-1221 two weeks prior to any IP address change to avoid interruption in service.

Inbound to BSC:	Customer pushes file to BSC ☐	
	BSC FTP Server pulls file from customer ☐	Source Directory:
Outbound to customer:	Customer pulls from the BSC SFTP server☐	
	BSC FTP Server pushes to customer ☐	Source Directory:

Note: Blue Shield will email with your login ID and password for our secure FTP server, with a copy of our PGP public key, if applicable. Blue Shield will also request a login ID and Password if BSC will push or pull from the customer's server.

Blue Shield of California
Attn: EDI
4700 Bechelli Lane
Redding, CA 96002

Page 1

Fax to: EDI BSC at (530)351-6150
Email: EDI_BSC@blueshieldca.com

COMPLETE INFORMATION BELOW FOR HTTP/s CONNECTIVITY
Transmission Mode:

Batch ☐	Real Time ☐

HTTP/s Connectivity Standards:

SOAP ☐	MIME ☐

Static DNS Name and/or Static IP Address & Data Delivery Method

Primary DNS Name and/or IP address**: (   ).(   ).(   ).(   )**
Secondary DNS Name and/or IP address: (   ).(   ).(   ).(   )

IP addresses must be static. For IP address not registered in the name of the trading partner, complete the IP Ownership Verification Form.

Static DNS Name and/or Static IP Address & Data Delivery Method

Primary DNS Name and/or IP address**: (   ).(   ).(   ).(   )**
Secondary DNS Name and/or IP address: (   ).(   ).(   ).(   )

IP addresses must be static. For IP address not registered in the name of the trading partner, complete the IP Ownership Verification Form.

NOTE: Notify Blue Shield of California at (800) 480-1221 two weeks prior to any IP address change to avoid interruption in service.

Note: Blue Shield will email with your login ID and password for our secure FTP server, with a copy of our PGP public key, if applicable. Blue Shield will also request a login ID and Password if BSC will push or pull from the customer's server.

Blue Shield of California
Attn: EDI
4700 Bechelli Lane
Redding, CA 96002

Page 2

Fax to: EDI BSC at (530) 351-6150
Email: EDI_BSC@blueshieldca.com