
Independence Administrators

HIPAA Transaction Standard Companion Guide

**Refers to the Implementation Guides
Based on ASC X12 Implementation
Guides, version 005010**

December 2013

Independence Administrators is an independent licensee of the Blue Cross and Blue Shield Association.

Preface

This Companion Guide (“Companion Guide”) refers to the v5010 ASC X12 Implementation Guides and associated errata adopted under HIPAA and clarifies and specifies the data content when exchanging electronically with Independence Administrators. Transmissions based on this Companion Guide, used in tandem with the v5010 ASC X12 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 X12 Implementation Guides adopted for use under HIPAA. This Companion Guide is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the Implementation Guides.

EDITOR'S NOTE:

This page is blank because major sections of a book should begin on a right-hand page.

Table of Contents

- 1. Introduction 6
 - 1.1 Scope 7
 - 1.2 Overview 8
 - 1.3 References 9
 - 1.4 Additional Information..... 9
- 2. Getting Started..... 9
 - 2.1 Working with Highmark, Inc. (“Highmark”)..... 9
 - 2.2 Trading Partner Registration.....11
 - 2.3 Certification and Testing Overview 14
- 3. Testing with the Payer..... 14
- 4. Connectivity with the Payer/Communications 14
 - 4.1 Process Flows..... 15
 - 4.2 Transmission Administrative Procedures..... 15
 - 4.3 Re-Transmission Procedures 15
 - 4.4 Communication Protocol Specifications..... 15
 - 4.5 Passwords..... 17
- 5. Contact Information..... 17
 - 5.1 Highmark EDI Operations..... 17
 - 5.2 EDI Technical Assistance..... 18
 - 5.3 Provider Services..... 18
 - 5.4 Applicable Websites/Email..... 18
- 6. Control Segments/Envelopes 18
 - 6.1 ISA-IEA 19
 - 6.2 GS-GE 22
 - 6.3 ST-SE 22
- 7. Payer-Specific Business Rules and Limitations
(837P, 837I, U277, 835, and 999) 23
- 8. Acknowledgments and Reports 23
- 9. Trading Partner Agreements 23
- 10. Transaction-Specific Information 23
- Appendices..... 24
 - 1. Implementation Checklist..... 24
 - 2. Business Scenarios..... 24
 - 3. Transmission Examples 24
 - 4. Frequently Asked Questions..... 24
 - 5. Change Summary 24

1. Introduction

This section describes the ASC X12 Implementation Guides (IGs) adopted under HIPAA and is detailed using tables. The tables contain a row for each segment where Independence Administrators has something additional, over and above the information in the IGs. This information can:

- Limit the repeat of loops or segments;
- Limit the length of a simple data element;
- Specify a subset of the IGs internal code listings;
- Clarify the use of loops, segments, composite, and simple data elements;
- Provide any other information tied directly to a loop, segment, composite, or simple data element pertinent to trading electronically with Independence Administrators.

In addition to the row for each segment, one or more additional rows are used to describe the Independence Administrators 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.

The following table specifies the columns and suggested use of the rows for the detailed description of the Companion Guide.

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
193	2100C	NM1	Subscriber Name			This type of row indicates that a new segment has begun. It is shaded at 10%. Notes or comments about the segment are entered in this cell.
195	2100C	NM109	Subscriber Primary Identifier		15	This type of row limits the length of the specified data element.
197	2100C	REF01	Reference Identification Qualifier	18, 49, 6P, HJ, N6		These are the only codes transmitted by Independence Administrators.

Page #	Loop ID	Reference	Name	Codes	Length	Notes/Comments
			Plan Network Identification Number	N6		This type of row is used when a note for a particular code value is required. For example, this note could state that value N6 is the default. Not populating the first three columns indicates that the code value belongs to the row immediately above it.
218	2110C	EB	Subscriber Eligibility or Benefit Information			
231	2110C	EB13-1	Product/ Service ID Qualifier	AD		This row illustrates how to indicate a component data element in the Reference column and also how to specify that only one code value is applicable.

1.1 Scope

Independence Administrators migrated X12 transactions from its current gateway to the gateway managed and maintained by Highmark, Inc., formerly referred to as Highmark Health Services, (“Highmark Gateway”) an independent company.

The purpose of this Companion Guide is to provide guidance when submitting standard electronic transactions for Independence Administrators business. This Companion Guide addresses how providers, or their business associates, conduct the following HIPAA standard electronic transactions: Health Care Claim: Professional (837P), Health Care Claim: Institutional (837I), and Health Care Claim Payment/Advice (835) with Independence Administrators through the Highmark Gateway. In addition, it addresses the proprietary Unsolicited 277 - Claim Acknowledgment Transaction (U277).*

This Companion Guide also applies to the above referenced transactions that are being transmitted to Independence Administrators through the Highmark Gateway by a health care clearinghouse.

An Electronic Data Interchange (EDI) trading partner is defined as any entity (provider, billing service, software vendor, employer group, or financial institution) that utilizes the Highmark Gateway to send or receive electronic data to or from Independence Administrators.

The Highmark Gateway supports standard electronic transactions adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and additional supporting transactions as described in this Companion Guide. Highmark EDI Operations supports transactions for multiple payers, including Independence Administrators.

**005010X Independence Administrators Unsolicited 277 Claim Acknowledgment Transaction (U277) is the Independence Administrators proprietary functional acknowledgment for ANSI 837 claims transactions. Independence Administrators through the Highmark Gateway supports all listed transactions in batch mode.*

1.2 Overview

This Companion Guide includes information needed to commence and maintain communication exchange with Independence Administrators through the Highmark Gateway. This information is organized into the following sections:

- **Getting Started:** This section includes information related to system operating hours, provider data services, and audit procedures. It also contains a list of valid characters in text data. Information about trading partner authorization and an overview of the trading partner testing process is also included in this section.
- **Testing with the Payer:** This section includes detailed transaction testing information and other relevant information needed to complete transaction testing with Independence Administrators on the Highmark Gateway, if applicable.
- **Connectivity with the Payer/Communications:** This section includes information on the Highmark Gateway transmission procedures and communication and security protocols.
- **Contact Information:** This section includes telephone numbers and email addresses for support from Highmark EDI Operations.
- **Control Segments/Envelopes:** This section contains information needed to create the ISA-IEA, GS-GE, and ST-SE control segments for transactions to be submitted.
- **Payer-Specific Business Rules and Limitations:** This section contains information describing Independence Administrators business rules.
- **Acknowledgments and Reports:** This section contains information on all transaction acknowledgments. These include the Interchange Acknowledgment (TA1), Unsolicited - Claim Acknowledgment Transaction (U277), and the Implementation Acknowledgment for Health Care Insurance (999).
- **Trading Partner Agreements:** This section contains general information about and links to Provider and Clearinghouse/Vendor Trading Partner Agreements (collectively referred to herein as “Trading Partner Agreements”).

- **Transaction-Specific Information:** This section describes how IGs adopted under HIPAA will be detailed with the use of a table. The tables contain a row for each segment that has additional information that might supplement the IGs.

1.3 References

Trading partners must use the IGs adopted under the HIPAA Administrative Simplification Electronic Transaction rule and this Companion Guide for development of the EDI transactions. These documents will be made available through the EDI Trading Partner Business Center:

www.highmark.com/edi-ibc

Trading partners must use the most current national standard code lists applicable to the EDI transactions. The code lists may be accessed at the Washington Publishing Company website:

www.wpc-edi.com

The applicable code lists and their respective X12 transactions are as follows:

- Claim Adjustment Reason Codes and Remittance Advice Remark Codes (ASC X12/005010X221A1 Health Care Claim Payment/Advice [835])
- Provider Taxonomy Codes (ASC X12/005010X222A1 Health Care Claim: Professional [837P] and ASC X12/005010X223A2 Health Care Claim: Institutional [837I])

1.4 Additional Information

There is no additional information at this time.

2. Getting Started

2.1 Working with Highmark, Inc. (“Highmark”)

System Operating Hours

Highmark is available to handle EDI transactions 24 hours a day, 7 days a week, except during scheduled system maintenance periods.

It is highly recommended that trading partners transmit any test data during the hours that Highmark EDI Operations is available, 8:00 a.m. through 5:00 p.m. EST, Monday through Friday.

Audit Procedures

For purposes of conducting an audit for itself and/or Independence Administrators, Highmark may require access to the medical records used by the trading partner for submitting claims in accordance with the Trading Partner Agreement. The trading partner must ensure that input documents and medical records are retained and available for every automated claim for purposes of an

audit. Copies of trading partner documents are acceptable. The trading partner, not the billing agent, is held accountable for accurate records.

The audit conducted by Highmark consists of verifying a sample of automated claim input against medical records. Retention of records might also be checked. Compliance with reporting requirements is sample-checked to ensure proper coding technique is employed. Signature(s) on file records may also be verified.

In accordance with the Trading Partner Agreement, Highmark can request for itself and Independence Administrators, and the trading partner is obligated to provide, access to the records at any time.

Valid Characters in Text Data (AN, string data element type)

For data elements that are type AN, "string", Highmark can accept characters from the basic and extended character sets with the following exceptions:

Character	Name	Hex Value
!	Exclamation Point	(21)
>	Greater than	(3E)
^	Caret	(5E)
	Pipe	(7C)
~	Tilde	(7E)

These five characters are used by Highmark for delimiters on outgoing transactions and control characters for internal processing. Use of these characters can cause problems if encountered in the transaction data.

As described in the ASC X12 standards organization's Application Control Structure document (X12.6), a string data element is a sequence of characters from the basic or extended character sets and contains at least one non-space character. The significant characters are left justified. Leading spaces, when they occur, are presumed to be significant characters. In the actual data stream, trailing spaces should be suppressed. The representation for this data element type is AN.

Confidentiality/Security/Privacy

Trading partners, including health care clearinghouses, must comply with the HIPAA Electronic Transaction and Code Set standards and HIPAA Privacy and Security standards for all EDI transactions and confidentiality requirements as outlined in the Trading Partner Agreement.

Authorized Release of Information

When contacting Highmark EDI Operations concerning any EDI transactions, you will be required to confirm your trading partner information.

2.2 Trading Partner Registration

An Electronic Data Interchange (EDI) trading partner is defined as any entity (provider, billing service, software vendor, employer group, or financial institution) utilizing the Highmark Gateway to transmit or receive electronic standard transactions to or from Independence Administrators.

While Highmark EDI Operations accepts HIPAA-compliant transactions from any covered entity, HIPAA security requirements dictate that proper procedure is established to secure access to data. As a result, Highmark has a process in place to establish a trading partner relationship. That process has the following steps:

- The trading partner must identify Trading Partner Administrator and Delegate roles (see page 12 of this Companion Guide). Independence Administrators uses role-based security for transactions related to the maintenance of a trading partner relationship.
- The Trading Partner Administrator must complete an online application to receive from Highmark a DataStream Trading Partner ID associated with submitting transactions on behalf of Independence Administrators.
- The Trading Partner Administrator must agree to and electronically accept or otherwise submit the Trading Partner Agreement to Highmark. The Trading Partner Agreement establishes the legal relationship with Highmark and the requirements of that relationship. This is separate from a participating provider agreement.
- Once the Trading Partner Agreement is received by Highmark, the trading partner is sent a logon ID and password combination associated with the DataStream Trading Partner ID for use when accessing the Highmark Gateway for submission or retrieval of Independence Administrators transactions (“DataStream logon ID and password”). This DataStream logon ID is also used within EDI Interchanges as the ID of the trading partner. The Security section of this Companion Guide provides more detail about the maintenance of the DataStream logon ID and password by the trading partner.

Authorization Process

New trading partners that want to submit EDI transactions must submit an EDI Transaction Application to Highmark EDI Operations.

The EDI Transaction Application and the Trading Partner Agreement must be completed, electronically accepted and submitted by the Trading Partner Administrator who is an authorized representative of the organization submitting the EDI Transaction Application.

Highmark can terminate the Trading Partner Agreement after a sixty (60) day suspension period, without notice, if the trading partner’s account is inactive for a period of six (6) consecutive months, pursuant to the terms of the Trading Partner Agreement.

Complete and accurate reporting of information on the EDI Transaction Application ensures that the authorization process is completed in a timely manner. If you need assistance in completing the EDI Transaction Application contact your company's technical support area, your software vendor, or Highmark EDI Operations.

Upon completion of the authorization process, a DataStream logon ID and password are assigned to the trading partner. Highmark EDI Operations will authorize, in writing, the trading partner to submit production Independence Administrators EDI transactions.

Trading Partner Administrator and Trading Partner Delegate Roles

This section explains the Trading Partner Administrator ("Administrator") and Trading Partner Delegate ("Delegate") roles. Highmark EDI Operations will only make changes to the trading partner record if the change request is received from the authorized Administrator or Delegate.

- The "Administrator" is the primary representative of the trading partner entity (provider office, billing service, clearinghouse, etc.) that is authorized by the trading partner to conduct all electronic business on behalf of the trading partner, including entering into Trading Partner Agreements, modifying trading partner capabilities, and conducting inquiries about electronic transactions.
- The "Delegate" is a representative of the Trading Partner Administrator that has been authorized by the trading partner/Trading Partner Administrator to conduct certain activities on behalf of the trading partner such as, requesting the addition or deletion of affiliated providers or conducting inquiries about electronic transactions.
- The provider is a physician or allied health care provider credentialed and approved to provide covered services to Independence Administrators members and submit standard electronic transactions for such services to Independence Administrators for processing.
- The Administrator is required to submit a security question and an answer to this question when registering. The security answer is used to confirm and verify the identity of the Administrator prior to Highmark making any form changes on behalf of the trading partner.

The following table lists the rights that an Administrator, a Delegate, and a provider are authorized to perform:

Independence Administrators Trading Partner Role-Based Security Matrix

Rights	Administrator	Delegate	Provider
EDI Trading Partner Business Center Permissions			
New trading partner registration	✓		
New trading partner request	✓		
Update a trading partner's address information	✓		
Delete a trading partner	✓		
Update claim transactions	✓		
Update Administrator	✓		
Establish Delegate	✓		
Update Delegate	✓	✓	
Request for production	✓	✓	
Provider changes	✓	✓	✓
Update software vendor	✓	✓	
Other Permissions			
Receive EDI transaction support	✓	✓	✓
Request password change	✓	✓	

Where to Get Authorization Forms to Request a DataStream Trading Partner ID

To receive a DataStream Trading Partner ID, you must complete an online EDI Transaction Application and electronically agree to the terms of the Trading Partner Agreement. The EDI Transaction Application form and all other EDI request forms are available through the *Sign Up* section of the EDI Trading Partner Business Center website.

www.highmark.com/edi-ibc

Receiving ASC X12/005010X221A1 Health Care Claim Payment/Advice (835) Transactions Generated from the Payment Cycle (Batch)

To receive Health Care Claim Payment/Advice (835 remittance transactions) generated from the payment cycle in a batch process, trading partners need to request 835 remittance transactions by completing an *Update Claims Transactions* form through the *Update Trading Partners* section of the EDI Trading Partner Business Center website.

www.highmark.com/edi-ibc

Adding a New Provider to an Existing Trading Partner

Trading partners currently using electronic claims submission who wish to add a new provider to their DataStream Trading Partner ID should complete the *Provider Changes* form in the *Update Trading Partners* section on the EDI Trading Partner Business Center website, and select the option to *Add Provider*.

www.highmark.com/edi-ibc

Deleting Providers from an Existing Trading Partner

Trading partners who wish to delete a provider from their DataStream Trading Partner ID should complete the *Provider Changes* form in the *Update Trading Partners* section of the EDI Trading Partner Business Center website, and select the option to *Delete Provider*.

www.highmark.com/edi-ibc

Reporting Changes in Status

If trading partners need to change any other trading partner information, they must inform Highmark EDI Operations by completing the appropriate trading partner update form through the *Update Trading Partners* section of the EDI Trading Partner Business Center website.

www.highmark.com/edi-ibc

2.3 Certification and Testing Overview

Independence Administrators through Highmark Transactional Testing

Detailed payer testing requirements and procedures to be determined.

Claims Transactions

Detailed payer testing requirements and procedures to be determined.

3. Testing with the Payer

Detailed payer testing requirements and procedures to be determined.

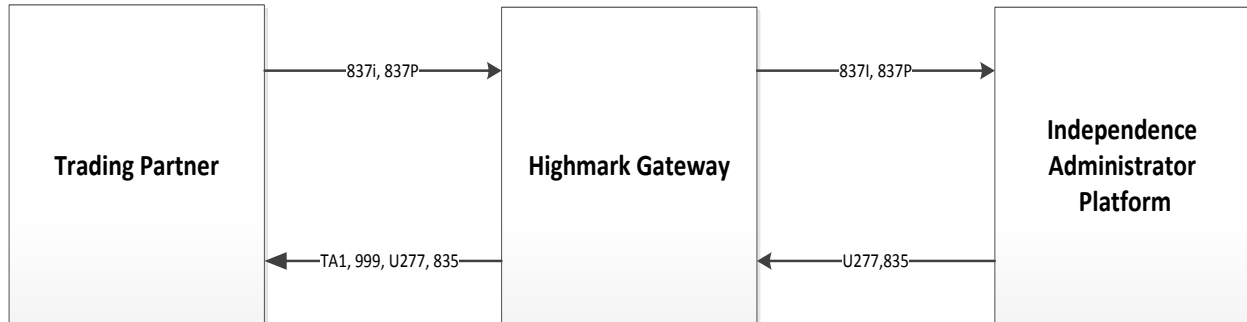
4. Connectivity with the Payer/Communications

Highmark offers Independence Administrators trading partners the following communication method for transferring data electronically:

- A secure https Internet connection available for transactions in batch mode.

4.1 Process Flows

Beginning in the fourth quarter of 2013, Independence Administrators will be migrating X12 transactions to the Highmark Gateway as illustrated in the diagram below:



Trading partners will submit and receive all transactions through the Highmark Gateway. The 999 Implementation Acknowledgment for Health Care Insurance transaction, TA1 Transaction Acknowledgment transaction, U277 Claim Acknowledgment transaction, and 835 Health Care Payment/Advice transaction are all returned to trading partners through the Highmark Gateway.

4.2 Transmission Administrative Procedures

This information will be communicated to the trading partner upon Highmark's receipt of the agreed-to Trading Partner Agreement.

4.3 Re-Transmission Procedures

Independence Administrators does not have specific re-transmission procedures. Trading partners can retransmit files at their discretion.

4.4 Communication Protocol Specifications

Internet

Highmark offers a secure File Transfer Protocol (SFTP) through "eDelivery" for conducting business with Independence Administrators. "eDelivery" is available for trading partners who submit or receive any HIPAA-compliant EDI transactions in batch mode.

Internet File Transfer Protocol (SFTP) through "eDelivery"

The Highmark Secure FTP Server ("eDelivery") provides an SFTP service over an encrypted data session providing "on-the-wire" privacy during file exchanges. This service offers an Internet accessible environment to provide the ability to exchange files with customers, providers, and business partners using a simple SFTP process in an encrypted and secure manner.

Any state-of-the-art browser can be used to access the Highmark Secure FTP Server. Browsers must support strong encryption (128 bit) and must allow

cookies for session tracking purposes. Once the browser capabilities are confirmed, the following are the general guidelines for exchanging files.

1. Launch your web browser.
2. Connect to the SFTP server at <https://ftp.highmark.com>.
3. The server prompts you for your DataStream logon ID and password. Use the DataStream logon ID/password that Highmark provided you as part of the trading partner authorization process for accessing this service. Enter the ID, tab to password field and enter the password.
4. Press “Enter” or click “OK”.
5. The server places you in an individual file space on the SFTP server. Other users cannot access your space and you cannot access the space of other users. You cannot change your space.
6. You need to change into the directory for the type of file you are uploading or downloading from the server.
7. By default, the file transfer mode is binary. This mode is acceptable for all data types. However, you can change between ASCII and binary file transfer modes by clicking the “Set ASCII”/ “Set Binary” toggle button.
8. Send Highmark a file. The following is an example of the submission of an electronic claim¹ transaction file:
 - a. Click the “hipaa-in” folder to change into that directory.
 - b. Click the **browse** button to select a file from your system to send to Highmark. A file finder box appears listing the files available on your system.
 - c. Select the file you want to send to Highmark and click **OK**. This returns you to the browser with the file name you selected in the filename window.
 - d. Click the **Upload File** button to transfer the file to Highmark. Once completed, the file appears in your file list.
9. Retrieve a file from Highmark. The following is an example of retrieval of an Implementation Acknowledgment For Health Care Insurance (999) file:
 - a. Click the “hipaa-out” directory. Your browser lists all the files available to you.
 - b. Click the “ack” directory.
 - c. Click the file you want to download. Your browser downloads the file. If your browser displays the file instead of downloading, click the **browser back** button and click the tools next to the file you want to receive. Select application/ octet-stream. You might be prompted with

¹Electronic claim includes both ASC X12/005010X222A1 Health Care Claim: Professional (837) and ASC X12/005010X223A2 Health Care Claim: Institutional (837) unless otherwise noted

the **Save As** file location window. Select a file location and click **Save** to download the file.

4.5 Passwords

Highmark EDI Operations assigns DataStream logon IDs and passwords to trading partners. EDI transactions submitted by unauthorized trading partners will not be accepted by the Highmark Gateway.

Trading partners should protect password privacy by limiting knowledge of the password to a key Administrator or their Delegates. Passwords should be changed regularly: upon initial usage and then periodically throughout the year. Also, the password should be changed if there are personnel changes in the trading partner office, or at any time the trading partner deems necessary. Trading partners must notify Highmark immediately if there is a violation of these DataStream logon ID and password requirements as required by the Trading Partner Agreement.

Password requirements include:

- Password must be eight characters in length.
- Password must contain a combination of both numeric and lower case alpha characters.
- Password cannot contain the logon ID.
- Password must be changed periodically.

Trading partners are directed to refer to the terms of their Trading Partner Agreement for any additional obligations they may have concerning logon IDs and passwords.

Password Change Requests

EDI Operations only performs a password reset if requested by an Administrator or Delegate.

If an Administrator or a Delegate provides the answer to their security question, EDI Operations can provide temporary passwords over the telephone. If the security answer is not provided, a temporary password is not given during the initial telephone call. In this case, the temporary password can be provided in a follow-up email or return telephone call using existing contact information on file at Highmark.

5. Contact Information

5.1 Highmark EDI Operations

Contact information for Highmark EDI Operations:

- Telephone Number: 1-800-992-0246
- Email Address: edisupport@highmark.com

When contacting Highmark EDI Operations, have your DataStream Trading Partner ID and DataStream logon ID available. These numbers facilitate the handling of your questions.

Highmark EDI Operations is available for questions from 8:00 a.m. to 5:00 p.m. EST, Monday through Friday.

5.2 EDI Technical Assistance

Contact information for Highmark EDI Operations:

- Telephone Number: 1-800-992-0246
- Email Address: edisupport@highmark.com

When contacting Highmark EDI Operations, have your DataStream Trading Partner ID and DataStream logon ID available. These numbers facilitate the handling of your questions.

Highmark EDI Operations is available for questions from 8:00 a.m. to 5:00 p.m. EST, Monday through Friday.

5.3 Provider Services

Non-EDI related inquiries should be handled through your existing channels of communication with Independence Administrators.

5.4 Applicable Websites/Email

EDI specifications, including this Companion Guide, will be accessible online in the *Resources* section of the EDI Trading Partner Business Center website:

www.highmark.com/edi-ibc

6. Control Segments/Envelopes

Interchange Control (ISA/IEA) and Function Group (GS/GE) envelopes must be used as described in the IGs. Independence Administrators expectations for inbound ISAs and a description of data on outbound ISAs are detailed in this chapter. Specific guidelines and instructions for GS and GE segments are contained in each transaction chapter of the Companion Guide.

Note: Highmark only supports one interchange (ISA/IEA envelope) per incoming transmission (file). A file containing multiple interchanges will be rejected for a mismatch between the ISA Interchange Control Number at the top of the file and the IEA Interchange Control Number at the end of the file.

For 5010 claim files, the ISA13 Control number must be unique for each submitted interchange. If the content of an interchange matches another interchange submitted within the last 14 days, the file is considered a duplicate and rejected with a TA1 Duplicate Interchange.

6.1 ISA-IEA

Delimiters

As detailed in the IGs, delimiters are determined by the characters sent in specified, set positions of the ISA header. For transmissions to Highmark EDI Operations (inbound transmissions), the following list contains all characters that can be accepted as a delimiter. Note that Line Feed, hex value "0A", is an acceptable delimiter.

Description	Hex value
StartOfHeading	01
StartofTeXt	02
EndofTeXt	03
EndOfTrans.	04
ENQuiry	05
ACKnowledge	06
BELL	07
VerticalTab	0B
FormFeed	0C
CarriageReturn	0D
DeviceControl1	11
DeviceControl2	12
DeviceControl3	13
DeviceControl4	14
NegativeAck	15
SYNchron.Idle	16
EndTransBlock	17
FileSeparator	1C
GroupSeparator	1D
RecordSeparator	1 E
!	21
"	22
%	25
&	26
'	27
(28
)	29
*	2A
+	2B
,	2C
.	2E
/	2F
:	3A
;	3B
<	3C
=	3D
>	3E

Description	Hex value
?	3F
@	40
[5B
]	5D
^	5E
{	7B
}	7D
~	7E

Note: “^” can be used as a Data Element Separator, but is not accepted as a Component Element Separator, Repeating Element Separator, or Segment Terminator.

Highmark uses the following delimiters in all outbound transactions. Note that these characters as well as the Exclamation Point, “!”, cannot be used in text data (type AN, Sting data element) within the transaction; refer section 2.1 Valid Characters in Text Data in this document.

Delimiter Type	Character Used	(Hex value)
Data element separator	^	(5E)
Component element separator	>	(3E)
Segment terminator	~	(7E)
Repeating element separator	{	(7B)

Data Detail and Explanation of Incoming ISA to Independence Administrators

Segment: ISA Interchange Control Header (Incoming)

Note: This fixed record length segment must be used in accordance with the guidelines in Appendix B of the IGs with the clarifications as follows:

Table 1: Data Element Summary

Loop ID	Reference	Name	Codes	Notes/Comments
ISA		Interchange Control Header		
	ISA01	Authorization Information Qualifier	00	Independence Administrators can only support code 00 - No Authorization Information present.
	ISA02	Authorization Information		This element must be space filled.
	ISA03	Security Information Qualifier	00	Independence Administrators can only support code 00 - No Security Information present.

Loop ID	Reference	Name	Codes	Notes/Comments
	ISA04	Security Information		This element must be space filled.
	ISA05	Interchange ID Qualifier	ZZ	Use qualifier code value "ZZ" Mutually Defined to designate a payer-defined ID.
	ISA06	Interchange Sender ID		Use the Independence Administrators assigned security logon ID. The ID must be left justified and space filled. Any alpha characters must be upper case.
	ISA07	Interchange ID Qualifier	33	Use qualifier code value "33". Independence Administrators only supports the NAIC code to identify the receiver.
	ISA08	Interchange Receiver ID	54704	Independence Administrators
	ISA13	Interchange Control Number		For 5010 claim files the ISA13 Control number must be unique for each submitted interchange. If the content of an interchange matches another interchange submitted within the last 14 days the file will be considered a duplicate and rejected with a TA1 Duplicate Interchange.
	ISA 14	Acknowledgment Requested	1	A TA1 segment is always returned when the incoming interchange is rejected due to errors at the interchange or functional group envelope.
	ISA15	Usage Indicator		The value in this element is used to determine the test or production nature of all transactions within the interchange.

Data Detail and Explanation of Outgoing ISA from Independence Administrators

Segment: ISA Interchange Control Header (Outgoing)

Note: The following table lists clarifications of Independence Administrators use of the ISA segment for outgoing interchanges:

Table 2: Data Element Summary

Loop ID	Reference	Name	Codes	Notes/Comments
ISA		Interchange Control Header		
	ISA01	Authorization Information Qualifier	00	Code 00 is sent - No Authorization Information present.
	ISA02	Authorization Information		This element must be space filled.
	ISA03	Security Information Qualifier	00	Code 00 is sent - no Security Information present.
	ISA04	Security Information		This element must be space filled.
	ISA05	Interchange ID Qualifier	33	Qualifier code value "33" is sent to designate that the NAIC code is used to identify the sender.
	ISA06	Interchange Sender ID	54704	Independence Administrators
	ISA07	Interchange ID Qualifier	ZZ	Qualifier code value "ZZ" is sent. Mutually defined to designate that an Independence Administrators-assigned proprietary ID is used to identify the receiver.
	ISA08	Interchange Receiver ID		The assigned ID is the trading partner's security logon ID. This ID is left-justified and space filled.
	ISA 14	Acknowledgment Requested		Independence Administrators always uses a 0 (No Interchange Acknowledgment Requested).
	ISA15	Usage Indicator		Independence Administrators provides T or P as appropriate to identify the test or production nature of all transactions within the interchange.

6.2 GS-GE

Functional group (GS-GE) codes are transaction specific.

6.3 ST-SE

Independence Administrators has no requirements outside the national transaction IGs.

7. Payer-Specific Business Rules and Limitations (837P, 837I, U277, 835, and 999)

During the transition, refer to EDI Services for Independence Administrators.

www.ibxtpa.com/providers/electronic_data_interchange.html

When the transition is completed, this document will be updated accordingly.

8. Acknowledgments and Reports

No additional requirements applicable.

9. Trading Partner Agreements

Provider Trading Partner Agreement

For use by professionals and institutional providers.

Clearinghouse/Vendor Trading Partner Agreement

For use by software vendors, billing services, or clearinghouses.

Trading Partners

An EDI trading partner is defined as any entity (provider, billing service, software vendor, employer group, or financial institution) utilizing the Highmark Gateway to transmit or receive electronic data to or from Independence Administrators.

Payers have 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 Trading Partner Agreement is with an entity or a part of a larger Agreement, between each party to the Agreement.

For example, a Trading Partner Agreement might specify the roles and responsibilities of each party to the Agreement in conducting standard electronic transactions.

10. Transaction-Specific Information

No additional requirements applicable.

Appendices

1. Implementation Checklist

Independence Administrators does not have an Implementation Checklist.

2. Business Scenarios

No business scenarios at this time.

3. Transmission Examples

No examples at this time.

4. Frequently Asked Questions

No FAQs at this time.

5. Change Summary

The items listed in the chart below were revised from the September 2013 version to this December 2013 version of the Companion Guide. Please note that there were no changes to transaction-specific information or codes.

Page(s)	Section	Description
7	Scope	Updated migration status, updated naming convention for Highmark, Inc.
9	Working with Highmark Inc. ("Highmark")	Updated naming convention for Highmark, Inc.
13	Trading Partner Registration	Added "Delegate" indicator for Update software vendor category