webMethods HIPAA Link Module Installation and User's Guide

Version 7.1

September 2010

webMethods

This document applies to webMethods HIPAA Link Module Version 7.1 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: ESTD-HIPAALink-IUG-71-20100920

Table of Contents

About This Guide

This guide describes how to install, configure, and use webMethods HIPAA Link Module to receive, parse, and validate all of the mandated HIPAA transactions and to respond with the appropriate acknowledgements.

To use this guide effectively, you should be familiar with:

- webMethods Integration Server and Integration Server Administrator, and understand the concepts and procedures described in *Administering webMethods Integration Server*.
- webMethods Trading Networks and webMethods EDI Module, and understand the concepts and procedures described in the various Trading Networks and EDI Module guides.
- webMethods Designer and webMethods Developer, and understand the concepts and procedures described in the webMethods Designer online help and the *Developing Integration Solutions: webMethods Developer User's Guide*.

  Note: Procedures for creating flow services and running webMethods HIPAA Link Module services are similar in Designer and Developer.

- My webMethods Server and its interface My webMethods, and understand the concepts and procedures described in the *Administering My webMethods Server* and *Working with My webMethods* guides.
- Have a basic knowledge of HIPAA standards and transactions as well as HIPAA terminology.

Document Conventions

Convention	Description
Bold	Identifies elements on a user interface.
Narrow font	Identifies storage locations for services on webMethods Integration Server, using the convention *folder.subfolder:service*.
UPPERCASE	Identifies keyboard keys. Keys you must press simultaneously are joined with a plus sign (+).
Italic	Identifies variables for which you must supply values specific to your own situation or environment. Identifies new terms the first time they occur in the text.
`Monospace font`	Identifies text you must type or messages displayed by the system.

Convention	Description
{}	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the {} symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Documentation Installation

You can download the product documentation using the webMethods Installer. Depending on the release of the webMethods product suite, the location of the downloaded documentation will be as shown in the table below.

For webMethods...	The documentation is downloaded to...
6.x	The installation directory of each product.
7.x	A central directory named _documentation in the main installation directory (webMethods by default).
8.x	A central directory named _documentation in the main installation directory (Software AG by default).

Online Information

You can find additional information about webMethods products at the locations listed below.

Note: The Empower Product Support Web site and the Software AG Documentation Web site replace Software AG ServLine24 and webMethods Advantage.

If you want to...	Go to...
Access the latest version of product documentation.	Software AG Documentation Web site http://documentation.softwareag.com

If you want to...	Go to...
Find information about product releases and tools that you can use to resolve problems. See the Knowledge Center to: ■ Read technical articles and papers. ■ Download fixes and service packs. ■ Learn about critical alerts. See the Products area to: ■ Download products. ■ Download certified samples. ■ Get information about product availability. ■ Access documentation for all supported versions of products. ■ Submit feature/enhancement requests.	Empower Product Support Web site https://empower.softwareag.com
■ Access additional articles, demos, and tutorials. ■ Obtain technical information, useful resources, and online discussion forums, moderated by Software AG professionals, to help you do more with Software AG technology. ■ Use the online discussion forums to exchange best practices and chat with other experts. ■ Expand your knowledge about product documentation, code samples, articles, online seminars, and tutorials. ■ Link to external Web sites that discuss open standards and many Web technology topics. ■ See how other customers are streamlining their operations with technology from Software AG.	Software AG Developer Community for webMethods http://communities.softwareag.com/webmethods

1 Concepts

What Is webMethods HIPAA Link Module?

webMethods HIPAA Link Module is a comprehensive and highly scalable solution that allows your organization to implement the HIPAA 4010, 4010 A1, and 5010 standards. This webMethods component provides out-of-the-box ability to receive, parse, and validate all of the mandated HIPAA transactions as well as generate the appropriate acknowledgements. HIPAA Link Module streamlines health care industry transactions by providing a solution for rapid and seamless integration of Providers, Payers, Routers, and Sponsors.

Important! HIPAA Link Module runs on top of webMethods EDI Module. When you install HIPAA Link Module, it changes the behavior of some of the functions of webMethods EDI Module to meet HIPAA standards. As a result, you must override EDI ID qualifiers to use those IDs in HIPAA Link Module (for example, in EDI the ID qualifier code 30 is "ISO 6523" but in HIPAA it is "Federal Tax ID"). For more information about adding and overriding EDI ID qualifiers, see *webMethods EDI Module Installation and User's Guide*.

If you plan to process both HIPAA-related and non-HIPAA related EDI documents, Software AG recommends that you set up the processing on different machines. If you prefer to use the same machine, be careful when setting up and testing to ensure that the processing for HIPAA and non-HIPAA related documents functions as anticipated.

webMethods HIPAA Link Module Features

HIPAA Link Module runs on top of webMethods Integration Server, webMethods Trading Networks, and webMethods EDI Module. HIPAA Link Module provides an easy, secure, and reliable solution for seamless integration with backhand systems and trading partners.

HIPAA Link Module provides support for the following.

- **Out-of-the-box HIPAA transactions**. This enables you to quickly implement production solutions for automating the many interactions between you and your trading partners. For a list of transactions that HIPAA Link Module supports, see "HIPAA Transactions that HIPAA Link Module Supports" on page 11.
- **Out-of-the-box validation**. HIPAA Link Module provides out-of-the-box validation through Level 6 as defined by WEDI-SNIP certification guidelines. You can customize HIPAA Link Module to add Level 7, trading partner-specific validation, if needed. In addition, you can choose to split HIPAA data into separate files after validation so that the valid data can be reused. You can also customize messages to send to partners based on validation results. For a description of validation levels, see "HIPAA Validation Levels" on page 14.

- HIPAA 4010, 4010 A1, and 5010 standards. HIPAA Link Module supports HIPAA 4010, 4010 A1, and 5010 standards out-of-the-box. With pre-packaged Integration Server and Trading Networks documents, you can easily transform an X12 document into an equivalent IS canonical document and vice versa.
- Large document processing. Instead of processing large HIPAA EDI documents all at once, HIPAA Link Module processes documents segment by segment to improve performance.
- Support for acknowledgements. HIPAA Link Module fully supports HIPAA-defined success/failure notification of envelope errors using TA1 technical acknowledgements. HIPAA Link Module also supports 997 functional acknowledgements and 999, 824, 277U, and 277A acknowledgements to communicate the validation results. HIPAA Link Module lets you create acknowledgements automatically with a validation service.
- Code sets. HIPAA transactions are also validated for code sets. With HIPAA Link Module, you receive periodic updates to the code sets and you can always be up to date with the latest code sets.
- Error reports. HIPAA Link Module generates detailed error reports in HTML and XML formats. You can send these reports in an e-mail message to a person in your enterprise or to a trading partner.
- Leveraging existing investments in enterprise solutions. You do so by accepting information from EDI-based systems to populate documents in HIPAA format.
- Transaction logging and audit trails. This ensures the integrity of all trading partner transactions. Automatic archival of transaction messages ensures non-repudiation of content.

HIPAA Transactions that HIPAA Link Module Supports

HIPAA Link Module supports the following HIPAA transactions and addenda:

Action	Enables users to...
270 Health Care Eligibility Benefit Inquiry	Send a Health Care Eligibility Inquiry, commonly known as 270, to submit an inquiry to the trading partner (generally an insurance company) to determine whether a patient is eligible for certain claim benefits. HIPAA Link Module supports: ■ 004010X092 (standard implementation) and 004010X092A1 (addendum) of version 4010 ■ 005010X279 of version 5010

Action	Enables users to...
271 Health Care Eligibility Benefit Response	Send a Health Care Eligibility Response, commonly known as 271, to submit a response to the trading partner stating whether the patient is eligible. The response document contains details such as eligibility status, maximum benefits, in-plan/out of plan benefits, and co-payments. HIPAA Link Module supports: ■ 004010X092 (standard implementation) and 004010X092A1 (addendum) of version 4010 ■ 005010X279 of version 5010
276 Health Care Claim Status Request	Send a Health Care Claim Status request, commonly known as 276, to request the current status of a specified claim. HIPAA Link Module supports: ■ 004010X093 (standard implementation) and 004010X093A1 (addendum) of version 4010 ■ 005010X212 of version 5010
277 Health Care Claim Status Response	Send a Health Care Claim Status Response, commonly known as 277, to transmit the current status within the adjudication process to the requester. When the status request does not uniquely identify the claim within the payer's system, the response may include multiple claims that meet the identification parameters that the requester supplies. HIPAA Link Module supports: ■ 004010X093 (standard implementation) and 004010X093A1 (addendum) of version 4010 ■ 005010X212 of version 5010
278 Health Care Services Review (Request and Response)	Send a Health Care Services Review (Request and Response), commonly known as 278, to handle informational inquiries and responses. The 278 can be exchanged between interested participants in a bi-directional inquiry/response mode of operation. This mode would allow a participant to inquire about existing certifications. HIPAA Link Module supports: ■ 004010X094 (standard implementation) and 004010X094A1 (addendum) of version 4010 ■ 005010X217 of version 5010

Action	Enables users to...
820 Payment Order/ Remittance Advice	Send a Payment Order/Remittance Advice, commonly known as 820, to validate a premium payment advice for a sender to move only money, to move money and detailed or summary remittance information, or to move only detailed or summary remittance information. HIPAA Link Module supports: ■ 004010X061 (standard implementation) and 004010X061A1 (addendum) of version 4010 ■ 005010X218 of version 5010
834 Benefit Enrollment and Maintenance	Send a Benefit Enrollment and Maintenance, commonly known as 834, to transfer enrollment information from the sponsor of the insurance coverage, benefits, or policy to a payer. HIPAA Link Module supports: ■ 004010X095 (standard implementation) and 004010X095A1 (addendum) of version 4010 ■ 005010X220 of version 5010
835 Claim Payment/Advice	Send a Claim Payment/Advice, commonly known as 835, to make a payment, send an Explanation of Benefits (EOB) remittance advice, or make a payment and send an EOB remittance advice from a health care payer to a health care provider, either directly or through a Depository Financial Institution (DFI). HIPAA Link Module supports: ■ 004010X091 (standard implementation) and 004010X091A1 (addendum) of version 4010 ■ 005010X221 of version 5010
837 Health Care Claims fall into three categories: Institutional, Dental, and Professional. HIPAA Link Module supports all three categories.	
837 Health Care Claim (Institutional)	Send a Health Care Claim (Institutional), commonly known as 837-I, to handle coordination of benefits (COB) in a totally EDI environment. HIPAA Link Module supports: ■ 004010X096 (standard implementation) and 004010X096A1 (addendum) of version 4010 ■ 005010X223A1 of version 5010

Action	Enables users to...
837 Health Care Claim (Dental)	Send a Health Care Claim (Dental), commonly known as 837-D, to handle coordination of benefits (COB) in a totally EDI environment. HIPAA Link Module supports: ■ 004010X097 (standard implementation) and 004010X097A1 (addendum) of version 4010 ■ 005010X224A1 of version 5010
837 Health Care Claim (Professional)	Send a Health Care Claim (Professional), commonly known as 837-P, to handle coordination of benefits (COB) in a totally EDI environment. HIPAA Link Module supports: ■ 004010X098 (standard implementation) and 004010X098A1 (addendum) of version 4010 ■ 005010X222 of version 5010

HIPAA Validation Levels

The HIPAA Implementation Guidelines specify six levels of message validation. HIPAA Link Module supports up to Level 6 out of the box. A seventh level can be added for trading partner-specific validation if needed.

Level	Description
1	Integrity. Validates the syntactical integrity of the X12 EDI document. Validation at this level includes testing for valid segments, segment order, element attributes, and so on.
2	Requirement. Validates using the syntax rules defined by the HIPAA Implementation Guidelines. Validation at this level includes testing for required repeat counts, used and not used codes, required or inter-segmental data elements, and so on.
3	Balancing. Validates to ensure for balanced field totals, record or segment counts, financial balancing of claims or remittance advice, and balancing of summary fields.
4	Situation. Validates for specific inter-segment situations that are described in the HIPAA Implementation Guidelines (for example, if A occurs, B must be populated). For example, if a transaction represents an accident claim, the date of the accident must be present.
5	Code Set. Tests that the transaction uses valid code set values as described in the HIPAA Implementation Guidelines (for example, CPT, NDC).

Level	Description
6	Product Types/Types of Service. Validates for specific requirements needed for a specialized health care service (for example, chiropractic, durable medical equipment [DME]). The special requirements are described in the HIPAA Implementation Guidelines.
7	Trading Partner-Specific. Validates for requirements that are unique to a specific trading partner. These requirements are not necessarily part of the HIPAA Implementation Guidelines. For information about adding this level of validation, see the section about transaction parameters in "Step 5: Create HIPAA Trading Partner Agreements" on page 31.

webMethods HIPAA Link Module Packages

HIPAA Link Module contains the following packages (sets of services and related files) that you install on Integration Server.

Package	Description
WmHIPAALink	Contains general application functionality and serves as the main holding area for application user interfaces. This package also contains shared components including implementations of common utilities, common validation services, and transport services. For detailed information about the HIPAA Link Module services, see Chapter 7, "WmHIPAALink Package Services".
WmHIPAALinkSample	(Optional package) Illustrates how to use HIPAA Link Module to process HIPAA messages to meet the HIPAA standard. You can use the sample services to process your own messages. For more information about installing this package, see "Installing the HIPAA Link Module Samples Package" on page 25. For more information about using this package, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide* that is included in the package.

IS Document Types

An IS document type contains a set of fields used to define the structure and type of data in a document (IData object). You can use an IS document type to specify input or output parameters for a service or specification. You can also use an IS document type to build a document or document list field and as the blueprint for pipeline validation and document (IData object) validation.

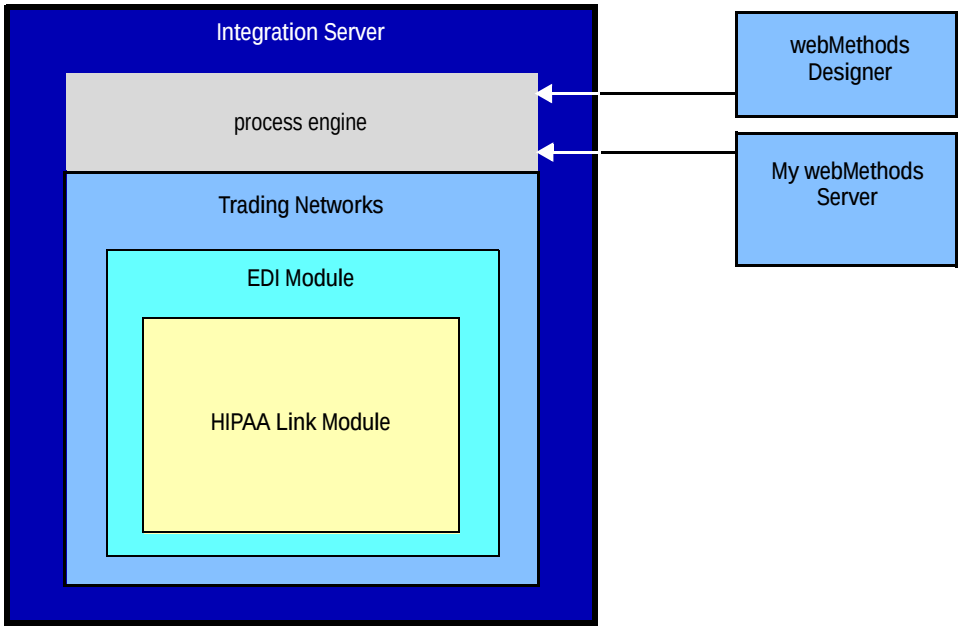
HIPAA Link Module provides flat file IS schemas and IS document types (in the WmHIPAALink package under the HIPAAFFSchema folder) for 4010 and 5010 HIPAA message types. You can use these schemas and documents to map the incoming HIPAA messages to backend IS documents and vice versa. The WmHIPAALinkSample package contains samples depicting the conversion of HIPAA messages to backend IS documents and vice versa.

For more information about IS document types, see *Developing Integration Solutions: webMethods Developer User's Guide* or *webMethods Designer Online Help*. For more information about the samples that convert HIPAA messages and IS documents, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide* that is included in the package.

webMethods HIPAA Link Module Architecture

The following diagram illustrates how HIPAA Link Module fits into the webMethods architecture.

Architecture and Components



Component	Description
Integration Server	Integration Server is the underlying foundation of the webMethods architecture. It processes requests from and relays responses to a back-end system. Among the services provided with Integration Server, HIPAA Link Module specifically uses services in the WmFlatFile package, which use flat file schemas to validate HIPAA transactions.

Component	Description
Trading Networks	Trading Networks is a webMethods component that enables your enterprise to link with other companies and exchanges to form a business-to-business trading network. For more information, see *Understanding webMethods B2B: webMethods Trading Networks Concepts Guide*.
EDI Module	webMethods EDI Module is a webMethods component that enables your enterprise to receive and process EDI documents. To use HIPAA Link Module, you use two packages of webMethods EDI Module: ■ WmEDI package, which contains the basic functionality that provides support for the EDI standard to the webMethods architecture. ■ WmEDIforTN package, which allows for the interaction between the WmEDI package and Trading Networks. This interaction allows you to use Trading Networks as a gateway for EDI document exchange.
webMethods Designer	At design time, you can use the Service Development perspective of webMethods Designer to create, view, modify, and delete services and IS document types. You can also use Designer to run services. Using Designer you can create process models that define the steps in a *business process* (also known as a *conversation*) for your HIPAA implementation. After you design the process models, you generate them to create the run-time elements (for example, flow services, triggers, and so on) that reside in Integration Server. The process engine facility of Integration Server executes the business processes (conversations) at run time. You also can use process models to process HIPAA documents. For more information, see *webMethods EDI Module Installation and User's Guide* and the webMethods Designer online help.
My webMethods Server	My webMethods Server is a run-time container for functions made available by webMethods applications such as Integration Server, Trading Networks, and HIPAA Link Module. For more information, see *Working with My webMethods*.
HIPAA Link Module	HIPAA Link Module is a webMethods component that adds support for the HIPAA standard.

Process Overview

To process HIPAA messages, you use the facilities provided by:

- HIPAA Link Module, which provides the HIPAA-related validation services
- webMethods EDI Module, which provides processing for EDI documents
- Trading Networks, which handles the routing of messages to trading partners

Additionally, you must add your own processing to do the following:

- Send HIPAA messages to your trading partners. If you are acting as a sender, you can use a Trading Networks delivery service to send a valid standard HIPAA message to your trading partner (acting as the receiver).
- Send the appropriate acknowledgements to the HIPAA messages. HIPAA Link Module provides built-in services that a receiver can invoke to generate acknowledgements. To send acknowledgements, you can use Trading Networks delivery features. For more information, see the Trading Networks documentation.

  The HIPAA Link Module sample illustrates how to use its built-in services. For more information about how to use the HIPAA Link Module built-in services, see Chapter 7, "WmHIPAALink Package Services" and *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.
- Process the HIPAA transactions to meet your specific needs. For example, you might want to map the data from a 834 Benefit Enrollment and Maintenance transaction to a back-end system document and send that document to your back-end system.

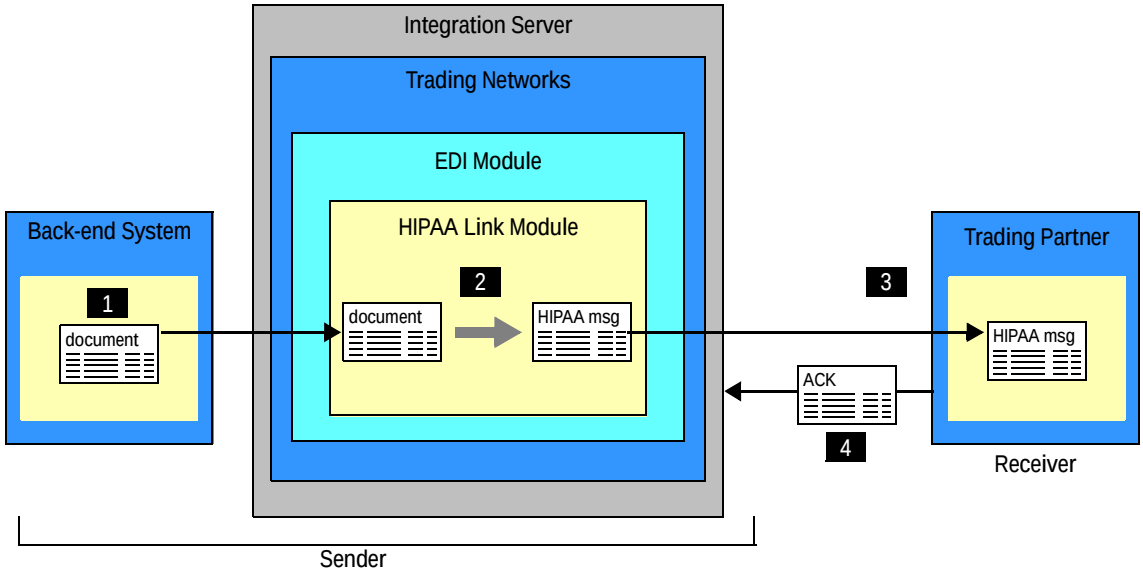
  The HIPAA Link Module sample illustrates how to map data to IS document types for processing on your back-end system. For more information about this process, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

To add your own processing, you can either use Trading Networks processing rules or you can use Designer to define a process model for a business process.

Sender-Side Processing

The sender forms a HIPAA message and sends it to a trading partner (that is, the *receiver* of the HIPAA message). The following diagram illustrates sender-side processing. For more information, see the table after the diagram.

Sender-side processing of HIPAA messages



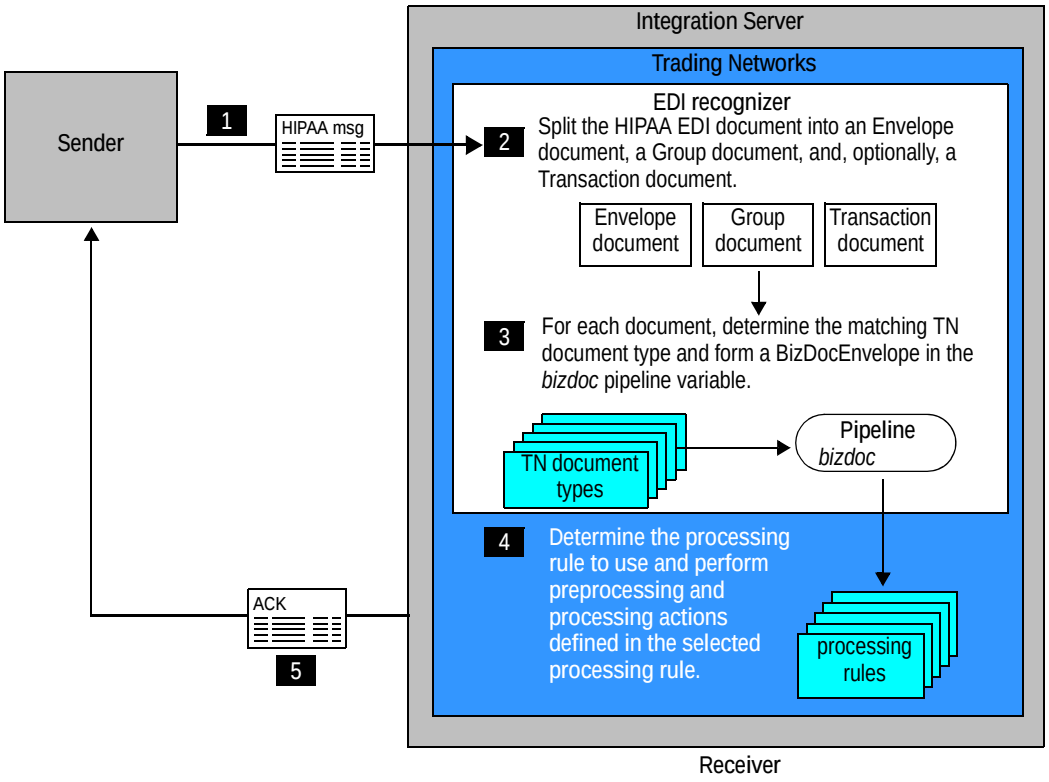
Step	Description
1	The back-end system sends a document to Integration Server. The document can be: ■ In an internal format used by the back-end system ■ A valid HIPAA message
2	The actions performed on Integration Server depend on the type of document sent: ■ If the back-end system sends documents in an internal format, you set up logic on Integration Server to map the data from the internal format document to a standard HIPAA message. For more information about how to do so, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*. ■ If the back-end system sends valid HIPAA messages, Integration Server needs only to send the HIPAA message to the receiver. You can use Trading Networks delivery features to send the HIPAA message to the receiver. For more information, see the Trading Networks documentation.

Step	Description
3	After a valid standard HIPAA message is available, use a Trading Networks delivery service to send the document to your trading partner (acting as the receiver). For more information, see the Trading Networks documentation.
4	The trading partner (acting as the receiver) sends an acknowledgement back to the sender. The sender processes this inbound acknowledgement. For information about how to process acknowledgements, see Chapter 6, "Processing HIPAA Acknowledgements".

Receiver-Side Processing

The following diagram illustrates receiver-side processing when using Trading Networks processing rules.

Receiver-side processing



Step	Description
1	Your trading partner creates a client that forms a HIPAA standard message and sends the HIPAA message to your Integration Server.
2	Integration Server receives the HIPAA message and sends it to Trading Networks for processing. Because the HIPAA message is an EDI document, Trading Networks passes the document to its EDI recognizer, which is a recognizer that is added to Trading Networks when you install webMethods EDI Module. The EDI recognizer splits the HIPAA message into separate documents. You define the level of documents (Envelope, Group, or Transaction) that you want the HIPAA message split into by setting a variable in an EDI trading partner agreement (EDITPA). For HIPAA processing, you *must* split at least at the Group level to form both Envelope and Group documents. For more information about EDITPAs and the EDITPA *splitOption* variable, see Chapter 3, "Configuring the webMethods HIPAA Link Module" in this guide and also see *webMethods EDI Module Installation and User's Guide*.
3	For each document (Envelope, Group, or Transaction) split from the original HIPAA message, the EDI recognizer uses the TN document types to determine the type of document (for example, X12 Envelope, X12 Group, or X12 4010 835). EDI Module provides the TN document types for EDI documents. You install the TN document types that you need. For more information, see "Step 1: Install TN Document Types for HIPAA Transactions" on page 28. The only exception is the TA1 technical acknowledgement, for which HIPAA Link Module automatically installs a flat file TN document type. After recognizing the type of document using TN document types, the EDI recognizer forms a *BizDocEnvelope* for the EDI document. The BizDocEnvelope is in the *bizdoc* pipeline variable. A BizDocEnvelope contains the original document (Envelope, Group, or Transaction) and includes additional information that Trading Networks requires for routing and processing the document. In other words, the BizDocEnvelope represents a routable Trading Networks transaction.

Step	Description
4	After the BizDocEnvelope is formed, the document undergoes regular Trading Networks processing. Trading Networks determines the processing rule to use to process the document and executes the processing rule. You create processing rules to define the processing you want performed on each type of document. For example, you set up processing for the Envelope document to validate the envelope and generate TA1 technical acknowledgements and 997 functional acknowledgements if appropriate. For more information about defining processing rules, see "Before You Can Process Inbound HIPAA Messages" on page 44.
5	Acknowledgements (for example, 997 and TA1) are sent back to the sender using Trading Networks delivery features. For more information, see the Trading Networks documentation.

2 Installing webMethods HIPAA Link Module

Overview

This chapter, in conjunction with the *Software AG Installation Guide*, explains how to install, upgrade, and uninstall webMethods HIPAA Link Module 7.1.

webMethods HIPAA Link Module requires webMethods Integration Server, webMethods Trading Networks, and webMethods EDI Module to be installed. For complete information about installing those products, see the *Software AG Installation Guide*.

Requirements

For a list of the operating systems and webMethods products that webMethods HIPAA Link Module 7.1 supports, see *webMethods eStandards Modules System Requirements*, available in the webMethods area of the Software AG Documentation Web site.

Installing HIPAA Link Module 7.1

This section provides only instructions that are specific to installing webMethods HIPAA Link Module 7.1. For complete instructions on using the webMethods Installer, see the *Software AG Installation Guide*.

To install HIPAA Link Module 7.1

1. If you are going to install webMethods HIPAA Link Module 7.1 on an already installed Integration Server, shut down Integration Server. For a list of the operating systems and webMethods products that webMethods HIPAA Link Module 7.1 supports, see "Requirements", above.
2. Download the webMethods Installer from the Empower Product Support Web site at https://empower.softwareag.com.
3. Start the webMethods Installer wizard.
4. In the **Release** list, choose the webMethods platform on which to install webMethods HIPAA Link Module. If you are going to install webMethods HIPAA Link Module on an existing Integration Server, select the platform that matches the release of that Integration Server. For example, if you are going to install webMethods HIPAA Link Module on a 7.1.3 Integration Server, select the 7.1-7.x platform.
5. Provide your Software AG Empower user name and password. The installer uses the user name and password to connect to the installer server and download the products for which you have purchased licenses.
6. Specify the installation directory to use. (The default is Software AG.)

7 In the product selection list, go to **eStandards > webMethods HIPAA Link Module 7.1** and select **Program Files**. You can also choose to install documentation and any required products indicated in the *webMethods eStandards Modules System Requirements*.

The installer installs the following components:

- webMethods Integration Server
- webMethods Trading Networks
- webMethods EDI Module
- webMethods HIPAA Link Module installed as the WmHIPAALink package in the *Software AG_directory*\IntegrationServer\packages directory

If Integration Server, Trading Networks, and webMethods EDI Module are already installed from a previous installation, the installer does not reinstall these products.

8 After installation completes, close the installer.

9 Start the Integration Server on which you installed HIPAA Link Module 7.1.

Installing the HIPAA Link Module Samples Package

The HIPAA Link Module samples package (WmHIPAALinkSample) contains the sample services to run HIPAA Link Module. The samples package is not installed with webMethods HIPAA Link Module 7.1. To download the WmHIPAALinkSample package, the installation procedure, and the *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*, go to the ESB & Integration forum on the Software AG Developer Community for webMethods at http://communities.softwareag.com/ecosystem/communities/public/Developer/webmethods/products/esb/ and see the Code Samples.

Uninstalling HIPAA Link Module 7.1

This section provides instructions that are specific to uninstalling webMethods HIPAA Link Module 7.1. For complete instructions on using the webMethods Uninstaller, see the *Software AG Installation Guide*.

To uninstall HIPAA Link Module 7.1

1 Shut down the Integration Server that hosts HIPAA Link Module 7.1.

2 Start the webMethods Uninstaller, as follows:

System	Instructions
Windows	In the **Add or Remove Programs** window, select the installation directory of the Integration Server on which HIPAA Link Module 7.1 is installed.

3 In the product selection list, go to eStandards > webMethods HIPAA Link Module 7.1. Choose to uninstall Program Files.

4 Restart the host Integration Server.

5 The uninstaller removes all HIPAA Link Module 7.1-related files that were installed into the *IntegrationServer_directory*\packages directory. However, the uninstaller does not delete files created after you installed the module (for example, user-created or configuration files), nor does it delete the module directory structure. You can go to the *IntegrationServer_directory*\packages directory and delete the HIPAA Link Module-related directory.

3 Configuring the webMethods HIPAA Link Module

Overview

This chapter describes how to set up the webMethods product suite so that you can send and receive HIPAA messages using the services in the webMethods HIPAA Link Module.

Important! The following procedure assumes that you already have installed webMethods Integration Server, webMethods Trading Networks, webMethods EDI Module, and webMethods HIPAA Link Module.

Step 1: Install TN Document Types for HIPAA Transactions

When Trading Networks receives a document, it uses its TN document types to determine the type of file it received. This is referred to as *document recognition.* In addition, the TN document type indicates the attributes that Trading Networks is to extract from the document. For more information about TN document types, see *Managing B2B Integrations: webMethods Trading Networks User's Guide* and *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

Note: When you install a TN document type, EDI Module also installs the corresponding flat file schema for the EDI transaction set. For more information about flat file schemas used for EDI documents, see the EDI Module documentation. For more information about flat file schemas in general, see the *Flat File Schema Developer's Guide*.

You use EDI Module to install TN document types for EDI documents. The TN document types are installed into Trading Networks. You need to install the TN document types for:

- The types of EDI transactions that you plan to use
- Various HIPAA acknowledgements: 999 (5010), 997 (4010, 5010), 824 (4050, 5010), and 277 (3070 for 277U, 4040 for 277A, 5010)

Note: You do *not* need to install a TN document type for the TA1 technical acknowledgement transaction. When you install EDI Module, the X12 TA1 TN document type is automatically installed into Trading Networks for the TA1 technical acknowledgement document.

To install TN EDI document types for HIPAA transactions

1 See the *webMethods EDI Module Installation and User's Guide* for complete information and the installation procedure on TN EDI document types and flat file schemas.

2 During the TN EDI document type installation procedure you will need to provide information for the standard, version, and transaction set. To do so, specify the following values:

For this field...	Specify...
Standard	X12
Version	4010
Transaction Set	Type of EDI document for which you want to install the associated TN document types, for example, 835. **Note:** You do not need to install a TN document type for the TA1 technical acknowledgement document. When you install a TN document type for a transaction set, the EDI Module automatically installs the TN document type for the Envelope and Group, if they are not already installed. As a result, the first time you install a TN document type for an X12 transaction, the X12 Envelope and X12 Group TN document types are installed.

3 Repeat steps 1 and 2 for each type of EDI document that you want to install.

Step 2: Define Profiles for Trading Partners

You need to define profiles for trading partners that will be exchanging HIPAA messages. Define profiles for the trading partners that will be identified as senders and receivers on the ISA (envelope) headers.

You create profiles use the Trading Networks Console. For steps to create profiles, see the chapter about creating partner profiles in *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

External ID Types in Profiles and EDI ID Qualifiers

In a Trading Networks profile, you specify external IDs to indicate how trading partners are identified within the HIPAA messages that they send. For example, if a trading partner uses a D-U-N-S number in a document, you define a DUNS external ID type in the Trading Networks profile and specify the trading partner's D-U-N-S number as the corresponding external ID.

For EDI documents, the external IDs correspond to the sender IDs and receiver IDs in the ISA headers of the EDI documents and the external ID types correspond to the EDI ID qualifiers (for example, 01 for a D-U-N-S number).

The table below lists the external ID types that the EDI Module installs into Trading Networks the first time you start the Integration Server Administrator after installing and enabling the EDI Module.

Trading Networks External ID Type	Corresponds to this EDI ID Qualifier
Carrier ID	27
DUNS	01
DUNS+4	14
Federal Tax ID	30
Fiscal Intermediary ID	28
Health Industry Number	20
Medicare ID	29
Mutually Defined	ZZ
NAIC Company Code	33

Note: You must override EDI ID qualifiers to use those IDs in HIPAA Link Module (for example, in EDI the ID qualifier code 30 is "ISO 6523" but in HIPAA it is "Federal Tax ID"). For more information about adding and overriding EDI ID qualifiers, see *webMethods EDI Module Installation and User's Guide*.

Step 3: Set Up Large Document Handling

To process large HIPAA documents using the HIPAA Link Module, you set up the webMethods EDI Module and webMethods Trading Networks to handle large documents, which temporarily persists documents to local disk for memory and performance optimization.

Configure the webMethods EDI Module

To configure the EDI Module to use large document handling, you must update specific EDI Module properties.

For more information about EDI large document handling and the properties to configure, see *webMethods EDI Module Installation and User's Guide*.

Configure webMethods Trading Networks

To configure webMethods Trading Networks to use large document handling, you must update specific Trading Networks and webMethods Integration Server properties.

For more information about Trading Networks large document handling and the properties to configure, see *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

Step 4: Create EDI Trading Partner Agreements

A trading partner agreement (TPA) is a Trading Networks object that defines how messages are exchanged between two trading partners. An EDI trading partner agreement (EDITPA) is a trading partner agreement that contains EDI Module-specific settings. The EDITPA contains a set of variables that you provide to tailor how the EDI Module splits HIPAA messages.

The EDI Module supports both partner-specific and default EDITPAs. A partner-specific EDITPA contains variables specific to a pair of trading partners where one is defined as the sender and the other the receiver. If a partner-specific EDITPA is not defined or if a value in a partner-specific EDITPA is not set, the EDI Module uses its default EDITPA. For more information about EDITPAs, see documentation for the EDI Module.

You must define EDITPAs for envelope sender/receiver pairs identified in the ISA headers of the HIPAA messages that you will exchange. You need to either:

- Use the default EDITPA for all envelope-level sender/receiver pairs.

  -OR-

- Create partner-specific EDITPAs for the envelope-level sender/receiver pairs.

For complete steps to create EDITPAs, see *webMethods EDI Module Installation and User's Guide*. The following table shows the EDITPA settings you should use with the EDI Module. The EDI Module does not use EDITPA variables that are not listed in the table. You can set the values of the EDITPA variables that are not listed to any value you choose.

EDITPA variable...	Value to use for the EDI Module
splitOption	Interchange, Group, or Transaction
GSRouting/routingMode	OFF The EDITPA *GSRouting/routingMode* variable indicates the value that you want the EDI Module to use for the sender and receiver, which the EDI Module puts in the Envelope, Group, and Transaction documents split from the HIPAA message. You must select OFF, which indicates that the EDI Module uses the sender and receiver from the ISA header for all types of documents.

Step 5: Create HIPAA Trading Partner Agreements

Whereas the EDI trading partner agreement defines how HIPAA messages are split, the HIPAA trading partner agreement (HIPAA TPA) defines how messages are validated and acknowledgements are generated.

A HIPAA TPA contains settings specific to HIPAA Link Module and based on the wm.estd.hipaa.rec:HipaaParameters and wm.estd.hipaa.rec:SeverityConfig IS document types. You modify these variables to tailor how messages are validated between two trading partners and how acknowledgements should be generated.

HIPAA Link Module provides a default TPA for an Unknown sender and receiver, which contains the default settings for all senders and receivers. You can edit this TPA or create a trading partner-specific TPA.

During the process of creating a partner-specific TPA, set the following values in the Agreement Details screen in Trading Networks Console:

- Identify the sender and receiver.
- Specify any value for Agreement ID.
- For IS Document Type, specify the value `wm.estd.hipaa.rec:HipaaParameters`.

For more information about creating and editing TPAs, see the chapter on defining and managing TPAs in *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

Note: If the TPA configuration contains errors, the default validation engine behavior is used to validate HIPAA messages between these partners. If errors occur, check the server log to determine the nature of the error and its resolution.

HIPAA Parameters

The following sections describe the parameters in the Interchange, Group, and Transaction sections of the TPA. The values for these parameters are specific to ANSI X12 standard document types.

Interchange Parameters

This section describes the parameters in the Interchange section of the TPA.

Parameter	Description
ControlVersion	Specifies the value of ISA segment, element 12 (for example, `00401` for version 4010 or `00501` for version 5010).
SenderID	Specifies the value of ISA segment, element 06. For the default HIPAA TPA for an Unknown sender, leave this parameter blank.
SenderQualifier	Specifies the value of ISA segment, element 05. For the default HIPAA TPA for an Unknown sender, leave this parameter blank.

Parameter	Description
ReceiverID	Specifies the value of ISA segment, element 08. For the default HIPAA TPA for an Unknown receiver, leave this parameter blank.
ReceiverQualifier	Specifies the value of ISA segment, element 07. For the default HIPAA TPA for an Unknown receiver, leave this parameter blank.
TA1	Specifies when to generate a technical acknowledgement. Possible values are: ■ always - Always generate the acknowledgement. This is the default setting. ■ never - Never generate the acknowledgement. ■ error - Generate the acknowledgement only if there are errors during validation of input data. ■ data - Generate the acknowledgement based on the data item. If there is no such item, this option functions the same as always.

Group Parameters

This section describes the parameters in the Group section of the TPA.

Parameter	Description
997	Specifies when to generate a functional acknowledgement. Possible values are: ■ always - Always generate the acknowledgement. This is the default setting. ■ never - Never generate the acknowledgement. ■ error - Generate the acknowledgement only if there are errors during validation of input data.

Parameter	Description
999	Specifies when to generate an implementation acknowledgement. Possible values are: ■ always - Always generate the acknowledgement. This is the default setting. ■ never - Never generate the acknowledgement. ■ error - Generate the acknowledgement only if there are errors during validation of input data. Note: This parameter applies to version 5010 only.
VersionNumber	Specifies the value of GS segment, element 08. Note: Select only those version numbers that are related to the control version defined in the Interchange parameter. For example, if the Interchange parameter *ControlVersion* is set to `00501`, select version numbers that start with "00501". Also, be sure not to add a duplicate version number. If you configure the same version number multiple times, validation will fail.

Transaction Parameters

This section describes the parameters in the Transaction section of the TPA. You must create an entry for each type of transaction.

Note: Add only those transactions that are related to the version number specified in the Group parameter *VersionNumber*. For example, if *VersionNumber* is set to `005010X279`, you can add transactions 270 and 271.

Parameter	Description
TransactionID	Specifies the transaction number. Valid values are 270, 271, 276, 277, 278-Req, 278-Res, 820, 834, 835, and 837.

Parameter	Description
AcknowledgementOption	Specifies the type of acknowledgement document to be generated and when the document should be generated. Acknowledgement document types are 824 (generated for all transaction types), 277U (generated for 837 transactions in version 4010 only), and 277A (generated for 837 transactions). Possible values for each type of acknowledgement are: ■ always - Always generate the acknowledgement. This is the default setting. ■ never - Never generate the acknowledgement. ■ error - Generate the acknowledgement only if there are errors during validation of input data.
ecsFileName	Specifies the Electronic Claims Submission (ECS) guideline to use for validation: ■ If EDI data is being *processed*, the EDI data for the transaction is validated against this file. ■ If EDI data is being *created*, the XML data is validated based on this file. A default ECS file exists for each type of transaction. Validation is performed against either the default ECS file or a custom one. You may need to create a custom ECS file, for example, to add trading partner-specific validation (Level 7). To validate using the default ECS file, leave this parameter blank. To validate using a custom ECS file, place the custom ECS file in the following folder: *IntegrationServer_directory*\packages\WmHIPAALink\resources\EDIFECS\STANDARDS\HIPAA\Version\<*version folder*>\ Specify the file name (without the folder qualifier) in the *ecsFileName* parameter. Note: SpecBuilder generates the ECS file. For information about generating and modifying an ECS file, see the SpecBuilder documentation.
SeverityDefinition	Specifies the severity settings to use for validation. For details, see "Severity Definition Parameters", below.

Severity Definition Parameters

The Severity Definition section of the TPA defines the error severity categories and their names and values. The following table describes the parameters for configuring the error severity of WEDI-SNIP certification types. Using the Trading Networks Console, you can add a new row for each of the seven HIPAA validation levels to customize error severity definitions for each validation level.

Parameter	Description
ValidationLevel	Specifies the HIPAA validation level for which to define error severity settings. Possible values are 1 through 7. For detailed explanations of each validation level, see "Process Overview" on page 18.
Severity	Specifies the severity of the error. Possible values are: ■ Ignore - Input data is accepted and the acknowledgement is generated to reflect this. No error is logged in the reports. ■ Information - Input data is accepted and the acknowledgement is generated to reflect this. The error is logged in the reports as severity "Information." ■ Warning - Input data is accepted with error and the acknowledgement is generated to reflect this. The error is logged in the reports as severity "Warning." ■ Error - Input data is rejected and the acknowledgement is generated to reflect this. The error is logged in the reports as severity "Normal."
CustomErrorMessage	Specifies custom error message text to display along with the default message in the report.
ErrorIDs	Specifies the error IDs associated with the validation level, severity, and custom error message in the report.

4 Creating Clients that Send HIPAA Messages

Overview

You create an Integration Server client to send HIPAA messages to Integration Server. Examples of applications that might use clients to send HIPAA messages are:

- A back-end system (for example, SAP or Oracle Applications) that sends a HIPAA message
- An Integration Server that sends a HIPAA message to another server
- A trading partner that is not using webMethods software that sends a HIPAA message

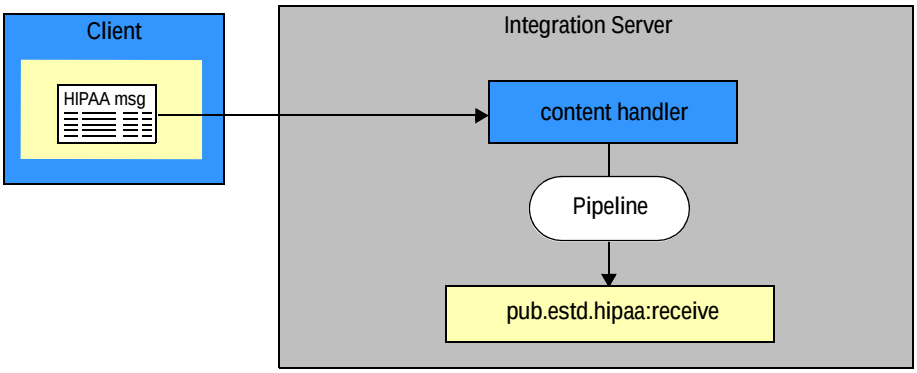
The client can use one of the following transports to send the HIPAA messages:

- HTTP or HTTPS
- FTP
- File Polling
- EDIINT AS1 or EDIINT AS2

For more information about using EDIINT, see *webMethods EDIINT Module Installation and User's Guide*. The rest of this section describes clients that use HTTP, HTTPS, FTP, or File Polling.

When a client sends a message to an Integration Server, the client must specify the content type of the data and identify the service to invoke to start the processing of the message. When Integration Server receives the message, it passes the message to the appropriate content handler based on the specified content type, and the content handler begins the processing, which includes creating the pipeline. For more information about creating clients, see *Developing Integration Solutions: webMethods Developer User's Guide*.

Client sends HIPAA messages to Integration Server



Content Type to Use

The content type your client should use to send the HIPAA messages to Integration Server depends on the type of HIPAA message that you are sending.

When your client sends....	It should use this content type
TA1 Technical Acknowledgement	application/x-wmflatfile
All other types of HIPAA messages	application/EDIStream Note: For backward compatibility, EDI Module also has content handlers to accept documents with the content types application/EDI and application/X12. With these content types, the EDI Module content handler must convert the document to a String and place it in the pipeline. This can potentially consume a lot of pipeline space and use a significant amount of memory. As a result, it is recommended that you use the content type application/EDIStream because it conserves system memory.

Service the Client Invokes

After the content type handler forms the pipeline, it invokes the service that the client specifies. Your client should invoke the pub.estd.hipaa:receive service. How this service behaves depends on whether you are sending a TA1 technical acknowledgement transaction or another type of HIPAA transaction.

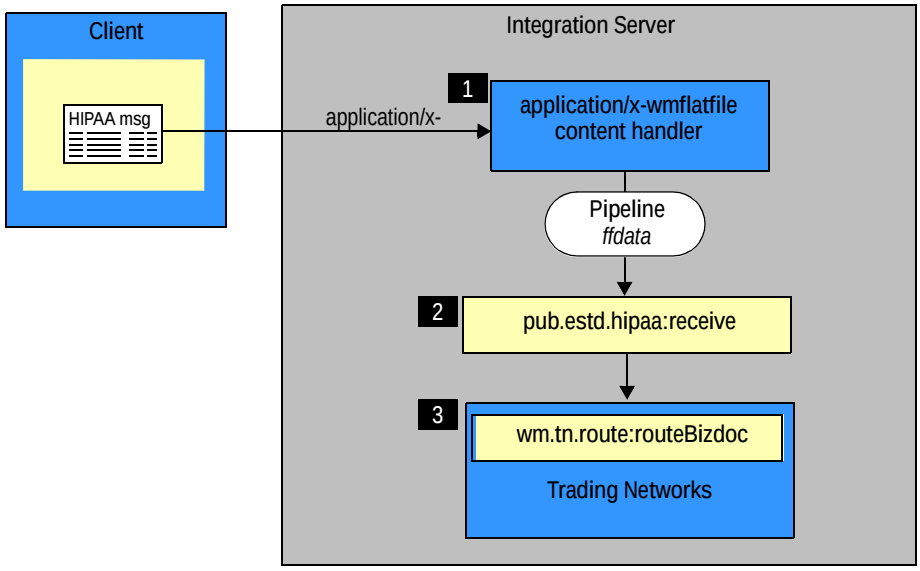
How pub.estd.hipaa:receive Handles TA1 Transactions

Because EDI Module does not support TA1 technical acknowledgement transactions, HIPAA Link Module adds this support. HIPAA Link Module adds support by treating the TA1 technical acknowledgement as a flat file document in Trading Networks rather than an EDI document.

When the client sends a TA1 technical acknowledgement message to Integration Server, the pub.estd.hipaa:receive service acts as a Trading Networks document gateway service. The gateway service places additional information about the TA1 technical acknowledgement in the pipeline that Trading Networks uses during its recognition processing. During recognition processing, Trading Networks matches the document to the X12 TA1 TN document type. It then proceeds with its normal processing. For more information about Trading Networks flat file processing, see *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

The following diagram illustrates the processing that occurs when a client sends a TA1 technical acknowledgement to Integration Server. For more information, see the table below the diagram.

Client sends a TA1 technical acknowledgement to Integration Server



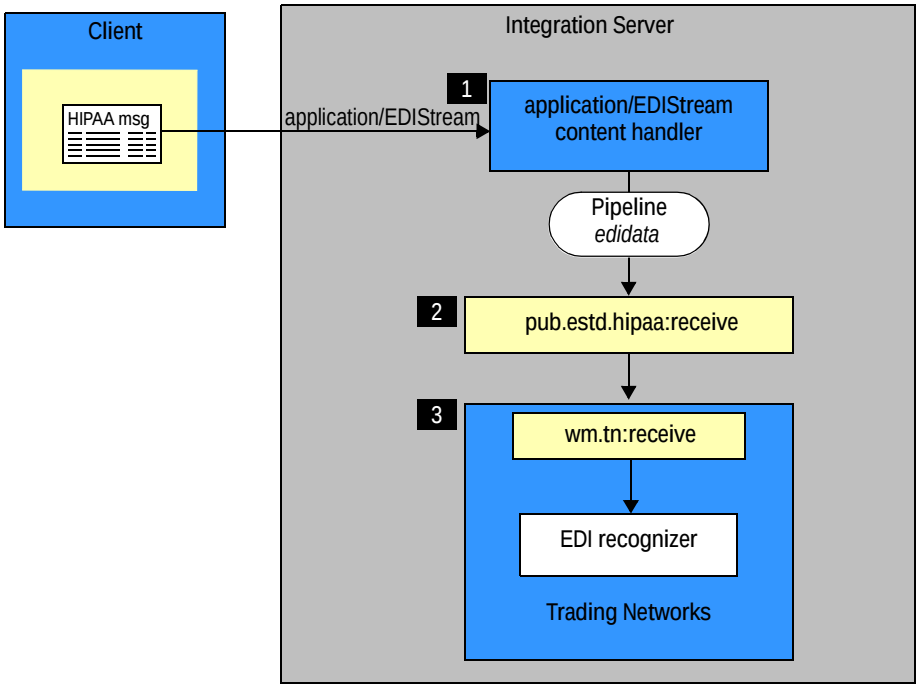
Step	Description
1	The client sends the HIPAA message with the content type application/x-wmflatfile to Integration Server, which in turn passes the HIPAA message to the application/x-wmflatfile content handler. The content handler performs initial processing, including forming the pipeline and placing the *ffdata* variable in the pipeline. The *ffdata* variable contains the HIPAA message data.
2	The content handler invokes the service that the client specified. For a HIPAA message, the client should specify the pub.estd.hipaa:receive service. The pub.estd.hipaa:receive service determines that the HIPAA message is a TA1 technical acknowledgement, and, because it is, the service acts as a gateway service used for Trading Networks flat file processing. The pub.estd.hipaa:receive service adds information to the pipeline. It also creates the BizDocEnvelope and sets the TN document type for the HIPAA message to X12 TA1. The service then invokes the wm.tn.route:routeBizdoc service.
3	The wm.tn.route:routeBizdoc service sends the HIPAA message directly to Trading Networks processing rules, bypassing document recognition. Trading Networks document recognition is bypassed because the pub.estd.hipaa:receive service already performed this function by creating the BizDocEnvelope and determining the TN document type to use for the HIPAA message.

How pub.estd.hipaa.receive Handles Other HIPAA Transactions

All HIPAA transactions other than a TA1 technical acknowledgement are treated as regular EDI documents. When the client sends any HIPAA message other than a TA1 technical acknowledgement to Integration Server, the pub.estd.hipaa:receive service invokes the wm.tn:receive service, which is the start of normal Trading Networks processing. Because the HIPAA message is an EDI document, Trading Networks passes the document to the EDI recognizer for processing. For more information about how EDI documents are processed in Trading Networks, see the EDI Module documentation.

The following diagram illustrates the processing when a client sends a HIPAA message other than a TA1 technical acknowledgement to Integration Server. For more information, see the table below the diagram.

Client sends a HIPAA message other than a TA1 technical acknowledgement to Integration Server



Step	Description
1	The client sends the HIPAA message with the content type application/EDIStream to Integration Server, which in turn passes the HIPAA message to the application/EDIStream content handler. The content handler performs initial processing, including forming the pipeline and placing the *edidata* variable in the pipeline. The *edidata* variable contains the HIPAA message data.
2	The content handler invokes the service that the client specified. For a HIPAA message, the client should specify the pub.estd.hipaa:receive service. The pub.estd.hipaa:receive service determines that the HIPAA message is *not* a TA1 technical acknowledgement, and because it is *not*, the service invokes only the wm.tn:receive service.
3	The wm.tn:receive service is the start of normal Trading Networks processing. Because the variable, *edidata*, is in the pipeline, Trading Networks passes the document to the EDI recognizer for EDI specific handling.

5 Processing HIPAA Messages Sent to Integration Server

Overview

This chapter describes how to set up Integration Server to process inbound HIPAA messages according to the HIPAA standard, including:

- Setting up Integration Server so that your services receive an inbound HIPAA message
- Validating the HIPAA message
- Responding with the appropriate acknowledgements (for example, TA1, 997, 824)

Important! This chapter describes how to implement processing to meet the HIPAA standard by validating and sending appropriate acknowledgements. It does *not* include how to process the actual transactions. To process the transaction (for example, map the data from a 834 Benefit Enrollment and Maintenance transaction to a back-end system document and send it to your back-end system), you perform functions as you would for any other EDI document. To learn more about processing inbound EDI documents including how to map data from an EDI document to a back-end system document, see *webMethods EDI Module Installation and User's Guide*. For more information about mapping HIPAA messages to IS document types and vice versa, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

Before You Can Process Inbound HIPAA Messages

Before setting up processing for inbound HIPAA message, do the following:

- Install the TN document types and flat file schemas for the HIPAA transactions that you want to process. For instructions, see "Step 1: Install TN Document Types for HIPAA Transactions" on page 28.
- Define profiles for the senders and receivers identified in the ISA headers of the HIPAA messages. For instructions, see "Step 2: Define Profiles for Trading Partners" on page 29.
- Define EDITPA settings for the sender/receiver pairs identified in the ISA headers of the HIPAA messages. For instructions, see "Step 4: Create EDI Trading Partner Agreements" on page 31.
- Define a HIPAA-specific TPA if required for the sender/receiver pairs identified in the ISA headers of the HIPAA message. For instructions, see "Step 5: Create HIPAA Trading Partner Agreements" on page 31.

Using Processing Rules to Process Inbound HIPAA Messages

As described in "Process Overview" on page 18, when Integration Server receives a HIPAA message, it passes the HIPAA message to Trading Networks. Because the HIPAA message is an EDI document, Trading Networks passes the document to the EDI recognizer for EDI Module-specific recognition processing.

The EDI recognizer splits the document based on the EDITPA *splitOption* variable. To perform processing to meet HIPAA standards, you must set the *splitOption* variable to Group or Transaction, so that the EDI recognizer forms at least the Envelope and Group documents from the HIPAA message.

This section describes how to set up processing rules for the Envelope and Group documents. You should set up one processing rule for an Envelope document and a second for a Group document.

Note: If you set the *splitOption* variable to Transaction, the EDI recognizer also will create Transaction documents that each contain a single transaction set from the HIPAA message. You define the specific processing that you want to perform against the transaction (for example, map the data to another document to send to your back-end system). This chapter does not describe how to do this processing. For more information, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

Defining a Processing Rule for an Envelope Document

To specify the processing you want to perform against the Envelope document, you define a processing rule. To meet the HIPAA standard, processing must include:

- Validating the ISA, GS, and ST segments
- Responding with appropriate acknowledgements (for example, TA1, 997, or 824)

The above processing is accomplished by using the Execute a service processing action to invoke a service that you create. HIPAA Link Module provides a sample service (wm.estd.hipaa.sample:processHipaaMessage) that you can use as a guideline. For more information about the sample, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

To create a processing rule for the Envelope

You create processing rules using the Trading Networks Console. For steps to create processing rules, see the chapter about processing rules in *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

1 **Set processing rule criteria.** Set the following criteria on the **Criteria** tab of the processing rule:

Criteria tab field	Set to...
Sender	Any Senders You can change this to select selected senders if you want.
Receiver	Enterprise It is important to select **Enterprise** for **Receiver** so that the processing rule is invoked only when you are receiving an Envelope document (and not when sending one).
Document Type	**Selected Document Types** and select the document type **X12 Envelope** The Envelope document will match the X12 Envelope TN document type. To ensure this processing rule is invoked *only* for the Envelope document, set the criteria to specify the X12 Envelope TN document type.

Important! If the envelope validation fails, the EDI recognizer does *not* split the Group and Transaction documents from the HIPAA message. As a result, Group and Transaction documents will *not* be processed. Only the Envelope document is passed to Trading Networks processing rules for processing, so your logic can handle the error and send a TA1 technical acknowledgement, if appropriate. For more information about how the HIPAA message is split into Envelope, Group, and/or Transaction documents, see "Process Overview" on page 18.

2 **Set processing actions.** On the **Action** tab of the processing rule:

   a Select **Perform the following actions**.

   b Select **Execute a service** and specify a service that you created to process the Envelope document.

   HIPAA Link Module provides a sample service (wm.estd.hipaa.sample:processHipaaMessage) that you can use as a guideline. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

For more information about the logic your service must perform to meet HIPAA standards and the built-in services provided by HIPAA Link Module that you can use as guidelines, see "Using Services to Process Inbound HIPAA Messages" on page 47.

Using Services to Process Inbound HIPAA Messages

This section describes the logic that you should include in the services you invoke from processing rules to process Envelope documents, including the actions that the service processing the Envelope document must take to meet the HIPAA standard.

Note: HIPAA Link Module provides a sample service (wm.estd.hipaa.sample:processHipaaMessage) that you can use as a guideline. For more information about the sample, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

---

1 Validate the envelope and perform HIPAA validation levels 1-7 according to the configuration options you selected in "Step 5: Create HIPAA Trading Partner Agreements" on page 31.

2 Process the message based on whether envelope validation errors occur:

- If envelope validation errors do occur, generate a negative TA1 technical acknowledgement and save it to the Trading Networks database. To send the acknowledgement to the trading partner who sent the HIPAA message being processed, use Trading Networks delivery features. For more information, see the Trading Networks documentation.

  Important! If the Validate pre-processing action determines that the envelope is *not* valid, the EDI recognizer does not split Group and Transaction documents from the HIPAA message. Only the Envelope document is passed to Trading Networks processing rules for further processing.

- If envelope validation errors do ***not*** occur, determine whether the sender requested a TA1 technical acknowledgement. If so, generate a TA1 technical acknowledgement and save it to the Trading Networks database. To send the acknowledgement to the trading partner who sent the HIPAA message being processed, use Trading Networks delivery features. For more information, see the Trading Networks documentation.

3 Generate the configured acknowledgements, such as a 997 functional acknowledgement, to report the outcome of the validation and save it to Trading Networks.

4 Using Trading Networks, send the acknowledgement to the trading partner who sent the HIPAA message that you are processing.

5 Optionally, you might want to update your back-end system based on information in the HIPAA message. To do so, you would map data from the HIPAA message to a document in the format that your back-end system requires, and then send the back-end system document to your back-end system. For more information about mapping data from HIPAA messages (EDI documents) to another format, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide* and *webMethods EDI Module Installation and User's Guide*.

The following table lists the built-in services that HIPAA Link Module includes to help you perform the above actions. For more information about these services, see Chapter 7, "WmHIPAALink Package Services".

Action	Built-in Service to Use
Validate the HIPAA message.	pub.estd.hipaa:validate
Recognize and persist the acknowledgements into the Trading Networks database.	pub.estd.hipaa:recognizeAcknowledgements
Recognize and persist the technical acknowledgement (TA1) into the Trading Networks database.	pub.estd.hipaa:recognizeTA1

6 Processing HIPAA Acknowledgements

Overview

This chapter describes how to set up Integration Server to process inbound HIPAA acknowledgements such as TA1 technical acknowledgements, 997 functional acknowledgements, and 999, 824, 277U, and 277A acknowledgements.

The HIPAA standard does not mandate how you are to process an acknowledgement. Typically, you would map the data from the acknowledgement to another document format, which you then can send to a back-end system. For more information about this mapping process, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

Before You Can Process Inbound HIPAA Acknowledgements

Before you set up processing for inbound HIPAA acknowledgements, do the following:

- Install the TN document types and flat file schemas for the X12 997 HIPAA transaction. For instructions, see "Step 1: Install TN Document Types for HIPAA Transactions" on page 28. The X12 TA1 TN document type is automatically installed for you when you install HIPAA Link Module.
- Define profiles for the senders and receivers identified in the ISA headers of the HIPAA acknowledgements. For instructions, see "Step 2: Define Profiles for Trading Partners" on page 29.
- Define EDITPA settings for the sender/receiver pairs identified in the ISA headers of the HIPAA acknowledgements. For instructions, see "Step 4: Create EDI Trading Partner Agreements" on page 31.
- Define a HIPAA-specific TPA if required for the sender/receiver pairs identified in the ISA headers of the HIPAA message. For instructions, see "Step 5: Create HIPAA Trading Partner Agreements" on page 31.

Defining Processing Rules for Inbound HIPAA Acknowledgements

This section describes how to set up processing rules for TA1 and 997 HIPAA acknowledgements. You should set up one processing rule for a TA1 technical acknowledgement and a second one for a 997 functional acknowledgement.

For other types of acknowledgements, you can create a processing rule that references the sample service wm.estd.hipaa.sample:processHipaaFA. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

Defining a Processing Rule for a TA1 Technical Acknowledgement

To specify the processing you want to perform against the TA1 technical acknowledgement, you define a processing rule. Typically, you will use the Execute a service processing action to invoke a service that you create to process the TA1 technical acknowledgement.

HIPAA Link Module provides the sample service wm.estd.hipaa.sample:processHipaaTA1 for you to use as a guideline. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

To create a processing rule for a TA1 technical acknowledgement

You create processing rules using the Trading Networks Console. For steps to create processing rules, see the chapter about processing rules in *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

Note: No specific settings are required on the Pre-Processing tab of the processing rule for a Group document.

1 Set processing rule criteria. Set the following criteria on the Criteria tab of the processing rule:

Criteria tab field	Set to...
Sender	Any Senders You can change this to selected senders if you want.
Receiver	Enterprise It is important to select Enterprise so that the processing rule is invoked only when you are receiving a TA1 technical acknowledgement (and not when sending one).
Document Type	Selected Document Type and select the document type X12 TA1 The TA1 technical acknowledgement will match the X12 TA1 TN document type. To ensure this processing rule is invoked *only* for the TA1 technical acknowledgement, set the criteria to specify the X12 TA1 TN document type.

2 Set processing actions. On the Action tab of the processing rule, do the following:

a Select Perform the following actions.

b Select Execute a service and specify a service that you created to process the TA1 technical acknowledgement.

HIPAA Link Module provides the sample service wm.estd.hipaa.sample:processHipaaTA1 for you to use as a guideline. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

For more information about the logic you might want to include in your service, see "Creating Services to Process HIPAA Acknowledgements" on page 53.

Defining a Processing Rule for a 997 Functional Acknowledgement

To specify the processing you want to perform against the 997 functional acknowledgement, you define a processing rule. Typically, you will use the Execute a service processing action to invoke a service that you created to process the 997 functional acknowledgement.

HIPAA Link Module provides the sample service wm.estd.hipaa.sample:processHipaaFA for you to use as a guideline. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

To create a processing rule for a 997 functional acknowledgement

You create processing rules using the Trading Networks Console. For steps to create processing rules, see the chapter about processing rules in *Building B2B Integrations: webMethods Trading Networks Administrator's Guide*.

Note: No specific settings are required on the Pre-Processing tab of the processing rule for a Group document.

1 Set processing rule criteria. Set the following criteria on the Criteria tab of the processing rule.

Criteria tab field	Set to...
Sender	Any Senders You can change this to selected senders if you want.
Receiver	Enterprise It is important to select Enterprise so that the processing rule is invoked only when you are receiving a 997 functional acknowledgement (and not when sending one).
Document Type	Selected Document Types and select the document type X12 4010 997 The 997 functional acknowledgement will match the X12 4010 997 TN document type. To ensure this processing rule is invoked *only* for the 997 functional acknowledgement, set the criteria to specify the X12 4010 997 TN document type.

2 Set processing actions. On the Action tab of the processing rule, do the following:

a Select Perform the following actions.

b Select Execute a service and specify a service that you created to process the X12 4010 997 document.

HIPAA Link Module provides the sample wm.estd.hipaa.sample:processHipaaFA service for you to use as a guideline. For details about this service, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

For more information about the logic you might want to include in your service, see "Creating Services to Process HIPAA Acknowledgements" on page 53.

Creating Services to Process HIPAA Acknowledgements

The HIPAA standard does not mandate how to process acknowledgements. You can create your service to perform any processing you require.

HIPAA Link Module provides the following sample services to illustrate how to process HIPAA acknowledgements:

- For a TA1 technical acknowledgement: the wm.estd.hipaa.sample:processHipaaTA1 service
- For a 997 functional acknowledgement and other types of acknowledgements: the wm.estd.hipaa.sample:processHipaaFA service

For details about these services, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

Processing you might want to perform is to update information in your back-end system based on the information in the acknowledgement. To do so, you would map data from the HIPAA acknowledgement to a document in the format that your back-end system requires, and then send that document to your back-end system. For more information about mapping data from HIPAA acknowledgements (EDI documents) to another format, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide* and *webMethods EDI Module Installation and User's Guide*.

7 WmHIPAALink Package Services

WmHIPAALink Package Services

This section describes the services available in the pub.estd.hipaa folder.

Note: Most services in the wm.estd.hipaa folder are for internal use only. For information about the sample services in this folder, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

pub.estd.hipaa:receive

This service receives, recognizes, and saves a HIPAA transaction or acknowledgement to the webMethods Trading Networks database.

Input Variables

ffdata Object (optional) The HIPAA transaction, 997 functional acknowledgement, or TA1 technical acknowledgement.

Output Variables

None.

Usage Notes

Use this service to receive a HIPAA real-time or batch transaction, a TA1 technical acknowledgement from a trading partner, or acknowledgements such as 997, 999, and so on. When sending the HIPAA message, the trading partner must set the content-type for the post to:

- application/x-wmflatfile when sending a TA1 technical acknowledgement
- application/EDIStream, application/EDI, or application/X12 when sending a HIPAA transaction or 997 functional acknowledgement

pub.estd.hipaa:recognizeAcknowledgements

This service recognizes and persists an acknowledgement to the Trading Networks database.

Input Variables

Ack String Acknowledgement data.

Output Variables

None.

pub.estd.hipaa:recognizeTA1

This service recognizes and persists a technical acknowledgement (TA1) to the Trading Networks database.

Input Variables

TA1	String Technical acknowledgement data.
prtIgnoreDocument	String Whether to create a new process model instance for the TA1 document with the generated conversation ID. Specify one of the following: ■ `true` - Do not create a process model instance. ■ `false` - Create a new process model instance to listen for the TA1 document using the generated conversation ID. Use this setting only if a process model exists to listen for the TA1 document.

Output Variables

None.

pub.estd.hipaa:validate

This service validates HIPAA 4010 and 5010 messages, splits valid and invalid HIPAA data from the input message into separate files after validation, returns the required acknowledgements, and formats acknowledgements and validation results in XML- and HTML-formatted reports.

Input Variables

hipaaDataFile	String Optional. The file path of the HIPAA message to be validated
ediDataContentPart	Document Optional. The *BizDocContentPart* document to be validated. For more information about the structure of this document, see the description for wm.tn.rec:BizDocContentPart in *webMethods Trading Networks Built-in Services Reference*.
split	String Optional. Whether to split valid HIPAA data and invalid HIPAA data into separate files after validation so that the valid data can be reused. Specify one of the following: ■ `true` - Split valid and invalid HIPAA data into separate files after validation. ■ `false` - Do not split the data into separate files. This is the default.

Output Variables

XML_Report	String Detailed report of the validation results in XML format.
HTML_Report	String Detailed report of the validation results in HTML format.
TA1	String List List of the technical acknowledgements corresponding to each interchange validated.
997	String List List of the functional acknowledgements corresponding to each functional group validated.
999	String List List of the implementation acknowledgements corresponding to each functional group validated. Note: This applies to version 5010 only.
277U	String List List of the Unsolicited Claim acknowledgements generated for 837 transactions. Note: This applies to version 4010 only.
277A	String List List of the Claim acknowledgements generated for 837 transactions.
824	String List List of each EDI Application Advice (824) message validated. 824 messages can be used for any transaction type to report errors for SNIP types 3 through 7.
validData	String Generated when *split* is set to `true`. Contains the data that the validation process determines as valid.
invalidData	String Generated when *split* is set to `true`. Contains the data that the validation process determines as invalid.

Usage Notes

Either *hipaaDataFile* or *ediDataContentPart* must be specified as input.

This service formats acknowledgements and validation results in HTML- and XML-formatted reports that contain the following information:

- Indication of whether the data file passed or failed validation
- Identifying information about the sender and receiver of the interchange, the interchange control number and version, the date and time the interchange was received, and the type of transaction the interchange contained
- If errors occurred, details about the rejected transaction, including:
  - Error ID
  - Detailed description of the error
  - Error data - the part of the data that caused the error during validation

- WEDI-SNIP certification type: the seven levels of validation as described in "Process Overview" on page 18
- Error severity
- Guideline properties related to the HIPAA specification

The service puts these reports in the pipeline. You can send these reports in an e-mail message to the appropriate person (for example, to correct errors).

You can also customize these reports to ignore certain validation level messages, to display a custom user message, and to prevent the generation of certain acknowledgements. You do so by configuring HIPAA TPA parameters. For details, see "Step 5: Create HIPAA Trading Partner Agreements" on page 31.