webMethods HIPAA Link Module Installation and User's Guide

Version 7.1

July 2011

webMethods

This document applies to webMethods HIPAA Link Module Version 7.1 SP1 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-71SP1-20110708

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 acknowledgments.

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 the appropriate Integration Server administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.
- webMethods Trading Networks and webMethods EDI Module, and understand the concepts and procedures described in the various Trading Networks and EDI Module guides.
- Software AG Designer and understand the concepts and procedures described in the appropriate Designer Process Development online help for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

  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 appropriate My webMethods administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5 and *Working with My webMethods* guides.
- Have a basic knowledge of HIPAA standards and transactions as well as HIPAA terminology.

Deprecation of webMethods Developer

webMethods Developer is deprecated and does not support all the features of webMethods Integration Server 8.2. Software AG recommends the use of Software AG Designer for service development.

Document Titles

Some Software AG document titles have changed during product releases. The following table will help you locate the correct document for a release on the Software AG Documentation Web site or the Empower Product Support Web site.

Documentation	Title
Designer Process Development online help	■ For Designer versions 8.2 and later, use *webMethods BPM Process Development Help*. ■ For Designer versions 8.0 and 8.1, use *webMethods Designer BPM Process Development Help*. ■ For Designer versions 7.1.1 and 7.1.2, use *webMethods Designer Process Development Help*.
Designer Service Development online help	■ For Designer versions 8.2 and later, use *webMethods Service Development Help*. ■ For Designer versions 7.2, 8.0, 8.0 SP1, and 8.1, use *webMethods Designer Service Development Help*.
Developer user's guide	■ For Developer 8.0 SP1 and later, use *Developing Integration Solutions: webMethods Developer User's Guide*. ■ For Developer 8.0 and earlier, use *webMethods Developer User's Guide*.
installation guide	■ For webMethods product suite 8.2 and later, use *Installing webMethods Products* and *Using the webMethods Installer.* ■ For webMethods product suite 8.0 SP1 and 8.1, use *Software AG Installation Guide*. ■ For webMethods product suite 8.0 and earlier, use *webMethods Installation Guide.*
Integration Server administration guide	■ For Integration Server 8.0 SP1 and later, use *Administering webMethods Integration Server*. ■ For Integration Server 8.0 and earlier, use *webMethods Integration Server Administrator's Guide*.
Integration Server built-in services reference guide	*webMethods Integration Server Built-In Services Reference*
Integration Server clustering guide	*webMethods Integration Server Clustering Guide*
Integration Server publish-subscribe guide	*Publish-Subscribe Developer's Guide*
logging guide	■ For Integration Server 8.0 SP1 and later, use *webMethods Audit Logging Guide*. ■ For Integration Server 8.0 and earlier, use *webMethods Logging Guide.*

Documentation	Title
My webMethods administration guide	■ For My webMethods Server 8.0.1 and later, use *Administering My webMethods Server*. ■ For My webMethods Server 8.0 and earlier, use *My webMethods Server Administrator's Guide.*
Optimize administration guide	■ For Optimize for Infrastructure 8.0 SP1 and later, use *Administering webMethods Optimize.* ■ For Optimize for Infrastructure 8.0 and earlier, use *webMethods Optimize Administrator's Guide.*
Optimize user's guide	■ For Optimize for Infrastructure 8.0 SP1 and later, use *Optimizing BPM and System Resources with BAM: webMethods Optimize User's Guide.* ■ For Optimize for Infrastructure 8.0 and earlier, use *webMethods Optimize User's Guide.*
Trading Networks administration guide	■ For Trading Networks 8.0 and later, use *Building B2B Integrations: webMethods Trading Networks Administrator's Guide.* ■ For Trading Networks 7.1.2, use *webMethods Trading Networks Administrator's Guide.*
Trading Networks built-in services reference guide	■ For Trading Networks 8.0 and later, use *webMethods Trading Networks Built-In Services Reference.* ■ For Trading Networks 7.1.2, use *webMethods Trading Networks Built-In Services Reference.*
Trading Networks concepts guide	■ For Trading Networks 8.0 and later, use *Understanding webMethods B2B: webMethods Trading Networks Concepts Guide.* ■ For Trading Networks 7.1.2, use *webMethods Trading Networks Concepts Guide.*
Trading Networks user's guide	■ For Trading Networks 8.0 and later, use *Managing B2B Integrations: webMethods Trading Networks User's Guide.* ■ For Trading Networks 7.1.2, use *webMethods Trading Networks User's Guide.*

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.
{}	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...
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
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

If you want to...	Go to...
■ 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, 4010A1, 5010 and 5010A standards. This webMethods component provides out-of-the-box functionality to receive, parse, and validate all of the mandated HIPAA transactions as well as generate the appropriate acknowledgments. HIPAA Link Module streamlines health care industry transactions by providing a solution for rapid and seamless integration of providers, payers, routers, and sponsors.

Note: 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 webMethods Integration Server, webMethods Trading Networks, and webMethods EDI Module. HIPAA Link Module provides an easy, secure, and reliable solution for seamless integration with external 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 13.
- 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 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 15.
- HIPAA 4010, 4010A1, 5010, and 5010A standards. HIPAA Link Module supports HIPAA 4010, 4010A1, 5010, and 5010A 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.
- Functional and technical acknowledgments. HIPAA Link Module fully supports HIPAA-defined success/failure notification of envelope errors using TA1 technical acknowledgments. HIPAA Link Module also supports 997 functional acknowledgments and 999, 824, 277U, and 277A acknowledgments to communicate the validation results. HIPAA Link Module lets you create acknowledgments automatically with a validation service.
- Code sets. HIPAA transactions are validated for code sets. With HIPAA Link Module, you receive periodic code set updates so that you can always be current.
- Error reports. HIPAA Link Module generates detailed error reports in HTML and XML formats. You can send these reports in an email message to someone in your enterprise or to a trading partner.
- Leveraging existing enterprise solutions. HIPAA Link Module allows you to accept information from other EDI-based systems to populate documents in HIPAA format.
- Transaction logging and audit trails. HIPAA Link Module ensures the integrity of all trading partner transactions with automatic archival of transaction messages.

HIPAA Transactions that HIPAA Link Module Supports

HIPAA Link Module supports the following HIPAA transactions and addenda:

Action	Enables users to...	HIPAA Link Module supports versions...
270 Health Care Eligibility Benefit Inquiry	Send a Health Care Eligibility Inquiry, also known as 270 to the trading partner (generally an insurance company) to determine whether a patient is eligible for certain claim benefits.	■ 004010X092 (standard) ■ 004010X092A1 (addendum) ■ 005010X279 (standard) ■ 005010X279A1 (addendum)
271 Health Care Eligibility Benefit Response	Send a Health Care Eligibility Response, also known as 271, response to the trading partner stating the patient's eligibility. The response document contains details such as eligibility status, maximum benefits, in-plan/out of plan benefits, and co-payments.	■ 004010X092 (standard) ■ 004010X092A1 (addendum) ■ 005010X279 (standard) ■ 005010X279A1 (addendum)

Action	Enables users to...	HIPAA Link Module supports versions...
276 Health Care Claim Status Request	Send a Health Care Claim Status request, also known as 276, to request the current status of a specified claim.	■ 004010X093 (standard) ■ 004010X093A1 (addendum) ■ 005010X212 (standard)
277 Health Care Claim Status Response	Send a Health Care Claim Status Response, also known as 277, to the requestor with the current status of the adjudication process. If the request matches more than one claim in the payer's system, the response may include multiple claims.	■ 004010X093 (standard) ■ 004010X093A1 (addendum) ■ 005010X212 (standard)
278 Health Care Services Review (Request and Response)	Send a Health Care Services Review (Request and Response), also known as 278, to handle informational inquiries and responses. 278 can be exchanged in a inquiry/ response operation mode to allow a participant to inquire about certifications.	■ 004010X094 (standard) ■ 004010X094A1 (addendum) ■ 005010X217 (standard)
820 Payment Order/ Remittance Advice	Send a Payment Order/ Remittance Advice, also known as 820, to validate a premium payment advice for a sender to move money, move money and remittance information, or only remittance information.	■ 004010X061 (standard) ■ 004010X061A1 (addendum) ■ 005010X218 (standard)
834 Benefit Enrollment and Maintenance	Send a Benefit Enrollment and Maintenance, also known as 834, to a payer to transmit enrollment information from the sponsor of the insurance coverage, benefits, or policy.	■ 004010X095 (standard) ■ 004010X095A1 (addendum) ■ 005010X220 (standard) ■ 005010X220A1 (addendum)
835 Claim Payment/Advice	Send a Claim Payment/Advice, also 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).	■ 004010X091 (standard) ■ 004010X091A1 (addendum) ■ 005010X221 (standard) ■ 005010X221A1 (addendum)

Action	Enables users to...	HIPAA Link Module supports versions...
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), also known as 837-I, to handle coordination of benefits (COB) in a totally EDI environment.	■ 004010X096 (standard) ■ 004010X096A1 (addendum) ■ 005010X223A1 (addendum) ■ 005010X223A2 (addendum)
837 Health Care Claim (Dental)	Send a Health Care Claim (Dental), also known as 837-D, to handle coordination of benefits (COB) in a totally EDI environment.	■ 004010X097 (standard) ■ 004010X097A1 (addendum) ■ 005010X224A1 (addendum) ■ 005010X224A2 (addendum)
837 Health Care Claim (Professional)	Send a Health Care Claim (Professional), also known as 837-P, to handle coordination of benefits (COB) in a totally EDI environment.	■ 004010X098 (standard) ■ 004010X098A1 (addendum) ■ 005010X222 (standard) ■ 005010X222A1 (addendum)

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, and element attributes.
2	Requirement. Validates the syntax rules meet the HIPAA Implementation Guidelines. Validation at this level includes testing for required repeat counts, used and unused codes, and required or inter-segmental data elements.
3	Balancing. Validates to ensure balanced field totals, record or segment counts, financial balancing of claims or remittance advice, and balancing of summary fields.
4	Situation. Validates specific situations 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 is required.

Level	Description
5	Code Set. Validates that the transaction uses valid code set values as described in the HIPAA Implementation Guidelines (for example, CPT, NDC).
6	Product Types/Types of Service. Validates specific requirements for a specialized health care service (for example, chiropractic, durable medical equipment [DME]). 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 33.

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 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. Use the sample services to process your own messages. For information about installing samples, see "Installing the HIPAA Link Module Samples Package" on page 25. For information about using samples, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

IS Document Types

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

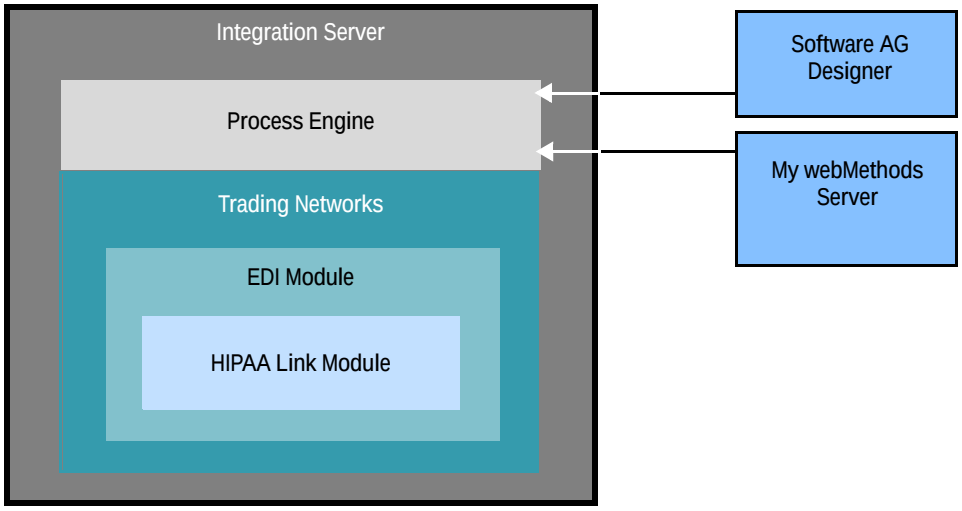
HIPAA Link Module provides flat file IS schemas and IS document types (in the WmHIPAALink package under the HIPAAFFSchema folder) for 4010 and 5010 HIPAA message types. Use these schemas and documents to map the incoming HIPAA messages to IS documents for external systems and vice versa. The WmHIPAALinkSample package contains samples to simulate these HIPAA message conversions.

For more information about IS document types, see the appropriate Designer Process Development online help for your release as noted in the "Document Titles" section of "About This Guide" on page 5. For more information about HIPAA messages samples see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

webMethods HIPAA Link Module Architecture

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

Architecture and webMethods Components



Component	Description
Integration Server	Integration Server is the underlying foundation of webMethods architecture. It processes requests from and relays responses to an external 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.
Trading Networks	Trading Networks enables your enterprise to link with other companies and exchanges to form a business-to-business trading network. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

Component	Description
EDI Module	EDI Module enables your enterprise to receive and process EDI documents. To use HIPAA Link Module, you use two of the EDI Module packages: ■ WmEDI package—contains the basic functionality that provides support for the EDI standard to webMethods architecture. ■ WmEDIforTN package—allows the interaction between the WmEDI package and Trading Networks, which serves as a gateway for EDI document exchange.
Software AG Designer	At design time, you can use the Service Development perspective of Software AG Designer to create, view, modify, and delete services and IS document types. Also use Designer to run services. You also use Designer to create process models that define the *business processes* (also known as a *conversation*) for your HIPAA implementation. When you generate the new process models, Designer creates the run-time elements (flow services and triggers) in Integration Server. Integration Server's process engine executes the business processes (conversations) at run-time. Also use process models to process HIPAA documents. For more information, see *webMethods EDI Module Installation and User's Guide* and the appropriate Designer Process Development online help for your release as noted in the "Document Titles" section of "About This Guide" on page 5.
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, use the facilities provided by:

- HIPAA Link Module provides the HIPAA-related validation services.
- EDI Module provides processing for EDI documents.
- Trading Networks 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 acknowledgments to the HIPAA messages.** HIPAA Link Module provides built-in services that a receiver can invoke to generate acknowledgments. To send acknowledgments, use Trading Networks delivery features. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

  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 an external system document and send that document to the downstream system.

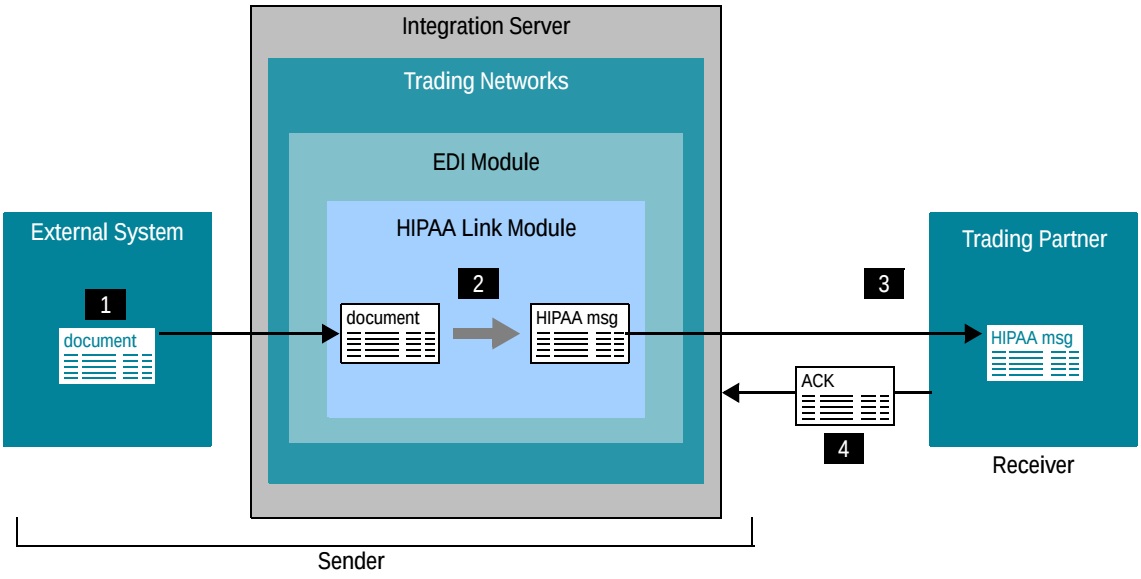
  The HIPAA Link Module sample illustrates how to map data to IS document types for processing by external systems. For information about this process, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*.

To add your own processing, use either Trading Networks processing rules or Designer to define custom process models and business processes.

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

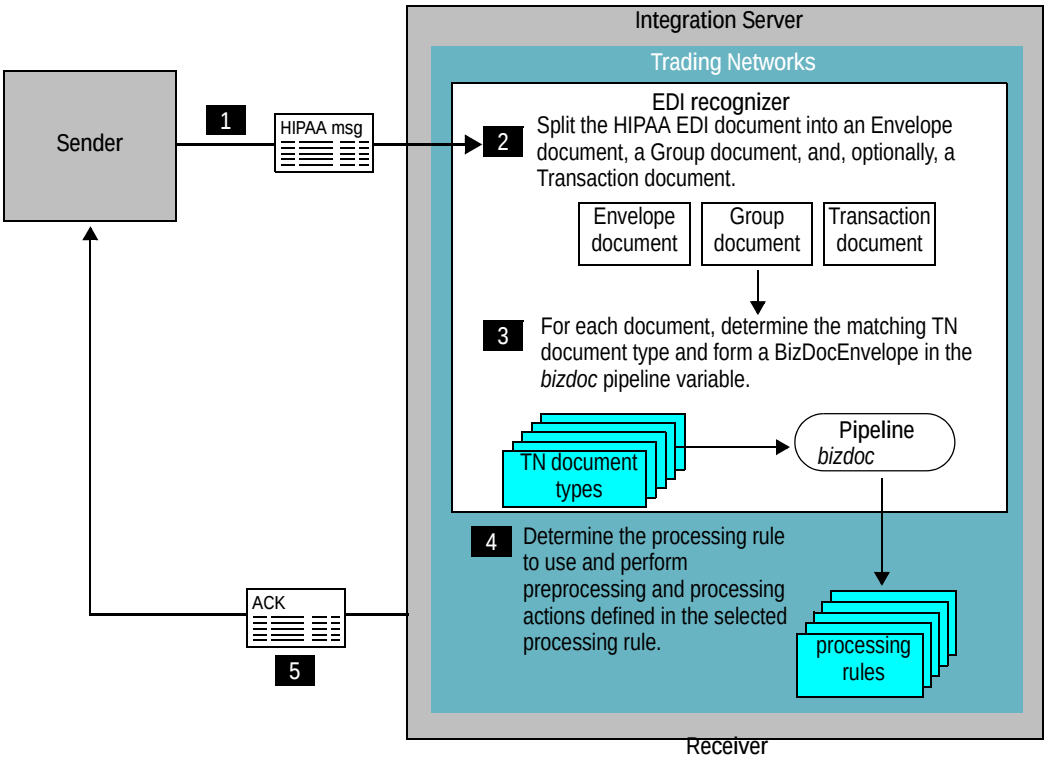


Step	Description
1	The external system sends a document to Integration Server, which can be: ■ In an internal format used by the external system ■ A valid HIPAA message
2	The actions performed on Integration Server depend on the type of document sent. If the external system sends: ■ Documents in an internal format, define logic on Integration Server to map the data from the internal format to a standard HIPAA message. For more information, see *webMethods HIPAA Link Module 7.1 Sample Package User's Guide*. ■ Valid HIPAA messages, Integration Server needs only to send the HIPAA message to the receiver. Use Trading Networks delivery features to send the HIPAA message. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.
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 appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.
4	The trading partner (acting as the receiver) sends an acknowledgment to the sender, who processes it accordingly. For information about how to process acknowledgments, see Chapter 6, "Processing HIPAA Acknowledgments".

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 EDI Module supplement to Trading Networks. The EDI recognizer splits the HIPAA message into separate documents. Set a variable in an EDI trading partner agreement (EDITPA) to define the level of documents (Envelope, Group, or Transaction) that you want the HIPAA message split into. 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*.

Step	Description
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 must install the TN document types that you need. For more information, see "Step 1: Install TN Document Types for HIPAA Transactions" on page 30. For the TA1 technical acknowledgment, however, 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.
4	After the BizDocEnvelope is formed, the document undergoes regular Trading Networks processing. Trading Networks determines which processing rule to execute on the document. For example, set up processing for the Envelope document to validate the envelope and generate TA1 technical acknowledgments and 997 functional acknowledgments, if appropriate. For more information about defining processing rules, see "Before You Can Process Inbound HIPAA Messages" on page 46.
5	Acknowledgments (for example, 997 and TA1) are returned to the sender using Trading Networks delivery features. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

2 Installing webMethods HIPAA Link Module

Overview

This chapter, along with *Software AG Installation Guide*, explains how to install, upgrade, and uninstall webMethods HIPAA Link Module 7.1 SP1.

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 *Software AG Installation Guide*.

Requirements

For a list of the operating systems and webMethods products that HIPAA Link Module 7.1 SP1 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 SP1

This section provides only instructions that are specific to installing HIPAA Link Module 7.1 SP1. For complete instructions on using the webMethods Installer, see *Software AG Installation Guide*.

To install HIPAA Link Module 7.1 SP1

1. Download the webMethods Installer from the Empower Product Support Web site at https://empower.softwareag.com.
2. If you are installing HIPAA Link Module 7.1 SP1 on an already installed Integration Server, shut down Integration Server.
3. Start the webMethods Installer wizard.
   - In the Release list, choose the webMethods release that includes the Integration Server version on which to install the module. For example, if you are installing HIPAA Link Module on Integration Server 7.1, select the 7.1 release.
   - Provide your Software AG Empower user name and password. The installer uses these to connect to the installer server and download the products for which you have purchased licenses.
   - Specify the installation directory to use (the default is Software AG.) If you are installing on an existing Integration Server, specify the webMethods installation directory that contains the host Integration Server. If you are installing both the host Integration Server and the module, specify the installation directory. The installer will install the module in the *IntegrationServer_directory*\packages directory.

- In the product selection list, select **eStandards > webMethods HIPAA Link Module 7.1 SP1**. You can also choose to install 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.

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

4. After installation completes, close the installer.
5. Start the Integration Server on which you installed HIPAA Link Module 7.1 SP1.

Installing the HIPAA Link Module Samples Package

The HIPAA Link Module samples package (WmHIPAALinkSample) contains the sample services. The samples package is not installed with HIPAA Link Module 7.1 SP1. To download the WmHIPAALinkSample package and *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.

Upgrading to HIPAA Link Module 7.1 SP1

This section describes how to upgrade and migrate the services created in HIPAA Link Module 7.1 to HIPAA Link Module 7.1 SP1.

To upgrade from HIPAA Link Module 7.1

1. Back up your existing HIPAA Link Module 7.1 installation and all custom packages that are used by HIPAA Link Module.
2. Using My webMethods Server, export all HIPAA Link Module 7.1 Trading Networks assets (profiles, TN document types, processing rules, TPAs and TN attributes) from Trading Networks. For information about exporting Trading Networks assets, see the appropriate administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

Note: Do not export the default HIPAA TPA (Sender/Receiver: Unknown and Agreement ID: HIPAA). HIPAA Link Module 7.1 SP1 automatically creates these, after which you can modify them, as needed.

3 Shut down Integration Server, if it is running.

4 Uninstall HIPAA Link Module 7.1. For instructions, see *webMethods HIPAA Link Module 7.1 Installation and User's Guide*.

Note: You must remove HIPAA Link Module related packages manually. To do so, navigate to the *IntegrationServer_directory*\packages directory and delete the WmHIPAALink and WmHIPAALink-related folders.

5 Install HIPAA Link Module 7.1 SP1 on a supported version of Integration Server. For instructions, see "Installing HIPAA Link Module 7.1 SP1" on page 24." For a list of supported Integration Server versions, see *webMethods eStandards Modules System Requirements*.

6 Start Integration Server, the Integration Server Administrator, and My webMethods Server.

7 Import into Trading Networks the custom HIPAA Link Module 7.1 Trading Networks assets that you exported in step 2. For instructions on importing Trading Networks assets, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

Uninstalling HIPAA Link Module 7.1 SP1

This section provides instructions that are specific to uninstalling HIPAA Link Module 7.1 SP1. For complete instructions on using the webMethods Uninstaller, see *Software AG Installation Guide*.

To uninstall HIPAA Link Module 7.1 SP1

1 Shut down the Integration Server that hosts HIPAA Link Module 7.1 SP1.

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 SP1 is installed.

3 In the product selection list, select eStandards > webMethods HIPAA Link Module 7.1 SP1.

4 Restart the host Integration Server.

5 The uninstaller removes all HIPAA Link Module 7.1 SP1-related files that were installed into the *IntegrationServer_directory*\packages directory. However, the uninstaller does not delete files that you created after you installed the module (for example, user-created or configuration files), nor does it delete the module directory structure. You can select 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 HIPAA Link Module.

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

Step 1: Install TN Document Types for HIPAA Transactions

When Trading Networks receives a document, it uses the TN document types to determine the file type. This is referred to as *document recognition.* Trading Networks also uses the TN document type to determine which attributes to extract from the document. For more information about TN document types, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 *Flat File Schema Developer's Guide*.

Use EDI Module to install TN document types for EDI documents into Trading Networks. You need to install the TN document types for:

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

To install TN EDI document types for HIPAA transactions

1 See *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, specify the following values:

For this field...	Specify...
Standard	`X12`
Version	`4010`

For this field...	Specify...
Transaction Set	Type of EDI document that corresponds to the TN document type that you want to install, for example, 835. EDI Module automatically installs the TN document types for both the Envelope and Group (if not already installed). For example, the installation of a TN document type for an X12 transaction includes the X12 Envelope and X12 Group TN document types.

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

Note: You do not need to install a TN document type for the TA1 technical acknowledgment document. The TA1 technical acknowledgment TN document type, X12 TA1, is automatically installed in Trading Networks when you install EDI Module.

Step 2: Define Profiles for Trading Partners

You must define profiles for each trading partner with whom you will exchange HIPAA messages. Define profiles for the trading partners that will be identified as senders and receivers on the ISA (envelope) headers.

Use My webMethods to create profiles. For information about creating profiles, see the the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

External ID Types in Profiles and EDI ID Qualifiers

In a Trading Networks profile, 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, 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).

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

Trading Networks External ID Type	Corresponds to this EDI ID Qualifier
Carrier ID	27
DUNS	01
DUNS+4	14

Trading Networks External ID Type	Corresponds to this EDI ID Qualifier
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: Configure Large Document Handling

To process large HIPAA documents using the HIPAA Link Module, configure EDI Module and Trading Networks to handle large documents. This feature temporarily persists documents to local disk for memory and performance optimization.

Configuring 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*.

Configuring Trading Networks

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

For more information about Trading Networks large document handling and the properties to configure, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 EDI Module splits HIPAA messages.

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 EDI Module.

You must define EDITPAs for envelope sender/receiver pairs identified in the ISA headers of the HIPAA messages that you exchange, either by:

- Using the default EDITPA for all envelope-level sender/receiver pairs.
- Creating 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 for EDI Module.

Note: EDI Module only uses the EDITPA variables listed in this table. You can set the values of the other EDITPA variables (not listed below) to any value you choose.

EDITPA variable...	Value to use for the EDI Module
splitOption	`Interchange`, `Group`, or `Transaction`
GSRouting/routingMode	`OFF` This variable indicates the value for sender and receiver that EDI Module should add to the Envelope, Group, and Transaction documents split from the HIPAA message. `OFF` indicates that 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 the acknowledgments are generated.

A HIPAA TPA contains settings specific to HIPAA Link Module, based on the wm.estd.hipaa.rec:HipaaParameters and wm.estd.hipaa.rec:SeverityConfig IS document types. Modify these variables to tailor how messages are validated between two trading partners and how HIPAA Link Module generates acknowledgments.

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.

In the Agreement Details screen in My webMethods, define the following values for a partner-specific TPA:

- 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 the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 an Unknown sender, leave this field blank to use the default HIPAA TPA.
SenderQualifier	Specifies the value of ISA segment, element 05. For an Unknown sender, leave this field blank to use the default HIPAA TPA.
ReceiverID	Specifies the value of ISA segment, element 08. For an Unknown receiver, leave this field blank to use the default HIPAA TPA.
ReceiverQualifier	Specifies the value of ISA segment, element 07. For an Unknown receiver, leave this field blank to use the default HIPAA TPA.
TA1	Specifies when to generate a technical acknowledgment: ■ always—Default. Always generate the acknowledgment. ■ never—Never generate the acknowledgment. ■ error—Generate the acknowledgment only if there are errors during validation of input data. ■ data—Generate the acknowledgment based on the data item. If there is no such item, this option is 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 acknowledgment: ■ always—Default. Always generate the acknowledgment. ■ never—Never generate the acknowledgment. ■ error—Generate the acknowledgment only if there are errors during validation of input data.
999	Specifies when to generate an implementation acknowledgment: ■ always—Default. Always generate the acknowledgment. ■ never—Never generate the acknowledgment. ■ error—Generate the acknowledgment 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". Be careful not to have multiple configurations for the same version or 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
AcknowledgmentOption	Specifies the type of acknowledgment to generate and when to generate it: ■ always—Default. Always generate the acknowledgment. ■ never—Never generate the acknowledgment. ■ error—Generate the acknowledgment only if there are errors during validation of input data. Acknowledgment document types are: ■ 824 (generated for all transaction types) ■ 277U (generated for 837 transactions, version 4010 only) ■ 277A (generated for 837 transactions)
ecsFileName	Specifies the Electronic Claims Submission (ECS) guideline to use for validation (either the default ECS file or a custom one). A default ECS file exists for each type of transaction. Create a custom ECS file, for example, to add trading partner-specific validation (level 7). Validation is based on the EDI data state. If the EDI data is: ■ Being *processed*, the EDI data is validated. ■ Being *created,* the XML data is validated. Define this ECS file validation parameter as follows: ■ Default validation—Leave the parameter blank. ■ Custom validation—Specify the file name (without the folder qualifier) and place the custom ECS file in: *IntegrationServer_directory*\packages\WmHIPAALink\resources\EDIFECS\STANDARDS\HIPAA\Version\<*version folder*>\ Note: SpecBuilder generates the ECS file. For information, 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 My webMethods, 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 "HIPAA Validation Levels" on page 15.
Severity	Specifies the severity of the error: ■ Ignore—Accept input data, generate an acknowledgment. Do not log an error in the reports. ■ Information—Accept input data and generate an acknowledgment. Log error in reports as severity, "Information." ■ Warning—Accept input data with error(s) and generate an acknowledgment. Log error in reports as severity, "Warning." ■ Error—Reject input data, generate an acknowledgment. Log the error 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:

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

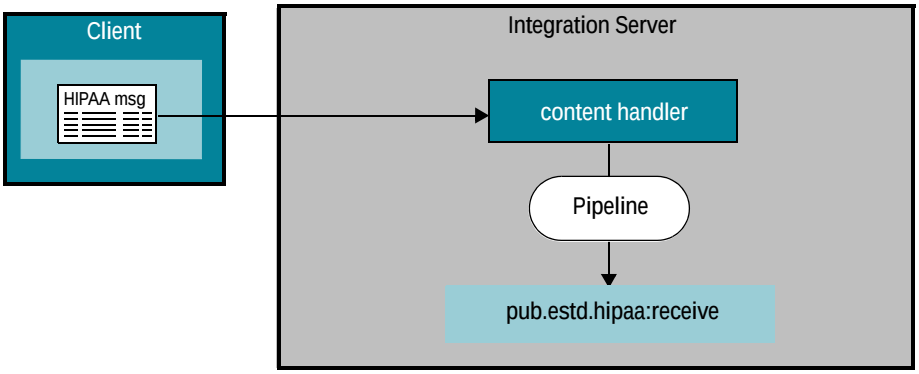
The client can use one of the following transport types to send the HIPAA messages:

- 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 remainder of this section describes clients that use HTTP, HTTPS, FTP, or File Polling.

When a client sends a message to Integration Server, the client must specify the content type of the data and identify which service to invoke to start processing the message. When Integration Server receives the message, it passes the message to the appropriate content handler based on the specified content type. The content handler, then, begins processing, which includes creating the pipeline. For more information about creating clients, see the appropriate Designer Process Development online help for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 send.

When your client sends....	It should use this content type
TA1 Technical Acknowledgment	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, 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. The behavior of this service depends on whether you are sending a TA1 technical acknowledgment transaction or another type of HIPAA transaction.

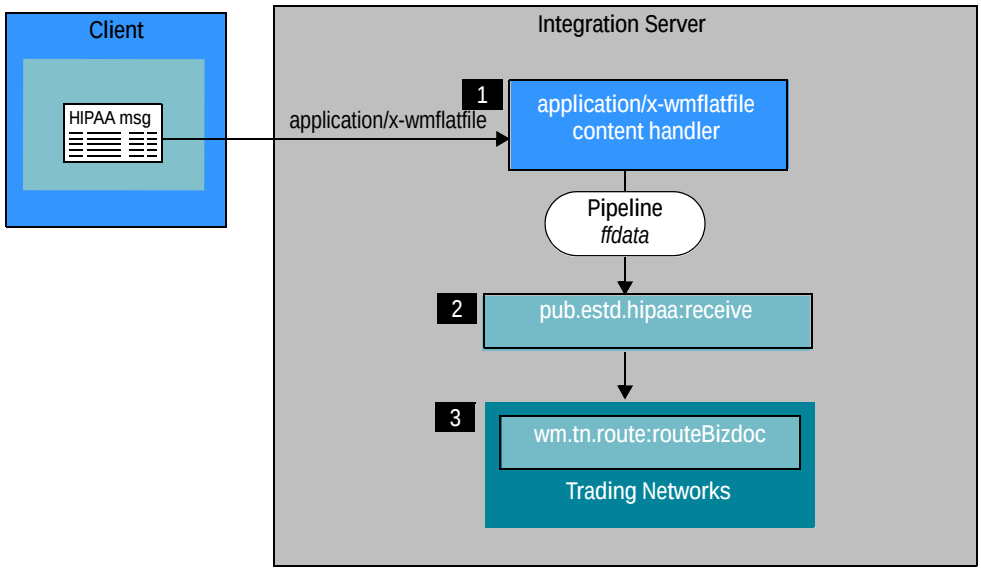
How pub.estd.hipaa:receive Handles TA1 Transactions

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

When the client sends a TA1 technical acknowledgment 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 acknowledgment in the pipeline that Trading Networks uses during its recognition processing. Trading Networks then matches the document to the X12 TA1 TN document type and proceeds with its normal processing. For more information about Trading Networks flat file processing, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

The following diagram illustrates the processing that occurs when a client sends a TA1 technical acknowledgment to Integration Server.

Client sends a TA1 technical acknowledgment 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 specified by the client. For a HIPAA message, the client should specify the pub.estd.hipaa:receive service. This service determines that the HIPAA message is a TA1 technical acknowledgment, and therefore, acts as a gateway service 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.

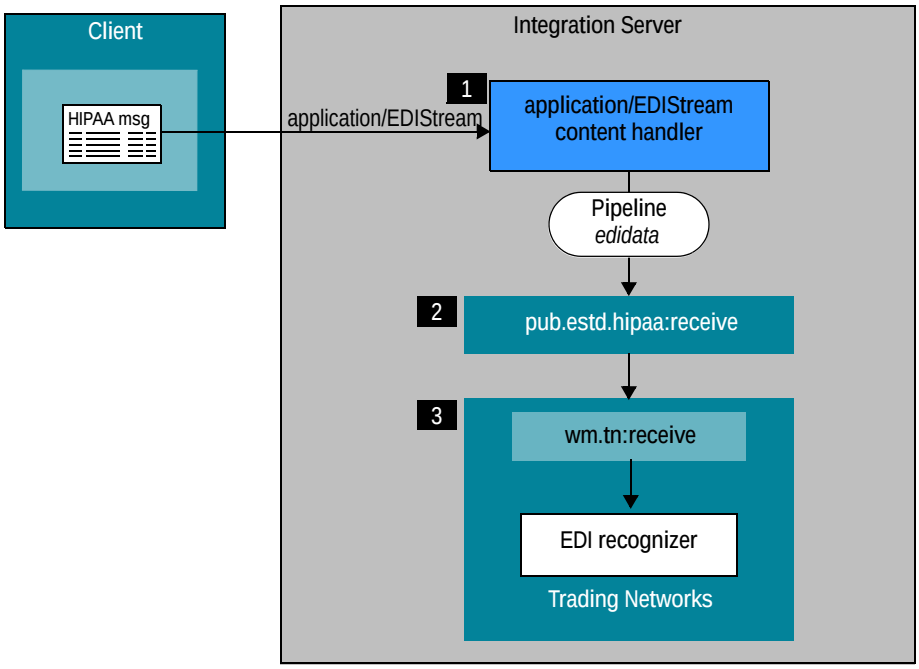
How pub.estd.hipaa.receive Handles Other HIPAA Transactions

All HIPAA transactions other than a TA1 technical acknowledgment are treated as regular EDI documents. When the client sends any HIPAA message other than a TA1 technical acknowledgment to Integration Server, the pub.estd.hipaa:receive service invokes

the wm.tn:receive service, starting 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 documentation for EDI Module.

The following diagram illustrates the processing when a client sends a HIPAA message that is not a TA1 technical acknowledgment to Integration Server. For more information, see the table below the diagram.

Client sends a HIPAA message other than a TA1 technical acknowledgment 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 specified by the client. For a HIPAA message, this should be the pub.estd.hipaa:receive service. The pub.estd.hipaa:receive service determines that the HIPAA message is *not* a TA1 technical acknowledgment, and therefore, 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 configure 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 acknowledgments (for example, TA1, 997, 824).

Important! This chapter describes processing to comply with HIPAA standards for validating and sending appropriate acknowledgments. It does *not* describe how to process the actual transactions. Transaction processing is the same as for any other EDI document. For information about processing inbound EDI documents, including how to map data from an EDI document to an external system document, see *webMethods EDI Module Installation and User's Guide*. For 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 30.
- 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 31.
- 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 32.
- 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 33.

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 comply with 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 configure processing rules for the envelope and group documents. You should set up one processing rule for an envelope document and another for a group document.

Note: If you set the *splitOption* variable to *transaction*, the EDI recognizer also creates transaction documents that each contain a single transaction set from the HIPAA message. Define how to process the transaction (for example, map the data to another document to send to your external 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 how to process the envelope document, you must define a processing rule that includes the following actions, in order to comply with the HIPAA standard:

- Validates the ISA, GS, and ST segments.
- Responds with appropriate acknowledgments (for example, TA1, 997, or 824).

To create a processing rule for the envelope

Create a processing rule in My webMethods. For information about how to create a processing rule, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 also select Selected Senders, if desired.
Receiver	Enterprise. Important! You must select Enterprise for this parameter so that the processing rule is only invoked when you are receiving an envelope document (and not when sending one).
Document Type	Selected Document Types. Select document type X12 Envelope Specify X12 Envelope as the TN document type for the envelope document to ensure the processing rule is only invoked when processing an envelope document.

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 are *not* processed. Only the envelope document is passed to Trading Networks for processing, so your logic can handle the error and send a TA1 technical acknowledgment, 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 do the following:

   a Select **Perform the following actions**.

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

   Use the HIPAA Link Module wm.estd.hipaa.sample:processHipaaMessage sample service as a guideline for creating your own service. 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 use 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 48.

Using Services to Process Inbound HIPAA Messages

This section describes the logic and processing actions that are required for services that process envelope documents, in order to comply with the HIPAA standard.

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 33.

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

- **If envelope validation errors occur**, generate a negative TA1 technical acknowledgment and save it to the Trading Networks database. To return the acknowledgment to the trading partner, use Trading Networks delivery features. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

  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 for further processing.

- **If envelope validation errors do *not* occur**, determine whether the sender requested a TA1 technical acknowledgment. If so, generate a TA1 technical acknowledgment and save it to the Trading Networks database. To return the acknowledgment to

the trading partner, use Trading Networks delivery features. For more information, see the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

3 Generate the configured acknowledgments, such as a 997 functional acknowledgment, to report the validation result and save it to Trading Networks.

4 Using Trading Networks, return an acknowledgment to the trading partner who sent the HIPAA message.

5 Optionally, you may want to update your external system based on information in the HIPAA message. To do so, map data from the HIPAA message to the data format required by your external system and then send the document to that 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 acknowledgments into the Trading Networks database.	pub.estd.hipaa:recognizeAcknowledgements
Recognize and persist technical acknowledgments (TA1) into the Trading Networks database.	pub.estd.hipaa:recognizeTA1

6 Processing HIPAA Acknowledgments

Overview

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

The HIPAA standard does not mandate how you process acknowledgments. Typically, you would map data from the acknowledgment to another document format, which you could then return to an external 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 Acknowledgments

Before you configure processing for inbound HIPAA acknowledgments, 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 30. The X12 TA1 TN document type is automatically installed with HIPAA Link Module.
- Define profiles for the senders and receivers identified in the ISA headers of the HIPAA acknowledgments. For instructions, see "Step 2: Define Profiles for Trading Partners" on page 31.
- Define EDITPA settings for the sender/receiver pairs identified in the ISA headers of the HIPAA acknowledgments. For instructions, see "Step 4: Create EDI Trading Partner Agreements" on page 32.
- 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 33.

Defining Processing Rules for Inbound HIPAA Acknowledgments

This section describes how to configure processing rules for TA1 and 997 HIPAA acknowledgments. You should define one processing rule for a TA1 technical acknowledgment and another one for a 997 functional acknowledgment.

For other types of acknowledgments, 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 Acknowledgment

To specify how to process a TA1 technical acknowledgment, you must define a processing rule and specify this rule in the Execute a service processing action for the TA1 technical acknowledgment.

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 acknowledgment

Create a processing rule in My webMethods. For information about how to create a processing rule, see the chapter about defining processing rules in the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 desired.
Receiver	Enterprise It is important to select Enterprise so that the processing rule is only invoked when you are receiving a TA1 technical acknowledgment (and not when sending one).
Document Type	Selected Document Type. Select the document type X12 TA1 Specify X12 TA1 as the TN document type for the TA1 technical acknowledgment to ensure the processing rule is only invoked for the TA1 technical acknowledgment.

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 acknowledgment.

HIPAA Link Module provides the wm.estd.hipaa.sample:processHipaaTA1 sample service for you to use as a guideline for designing your own service. 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 Acknowledgments" on page 55.

Defining a Processing Rule for a 997 Functional Acknowledgment

To define how to process a 997 functional acknowledgment, you must define a processing rule and specify this rule in the Execute a service processing action for the 997 functional acknowledgment.

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 acknowledgment

You create processing rules using My webMethods. For information about how to create processing rules, see the chapter about defining processing rules in the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.

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 desired.
Receiver	Enterprise It is important to select Enterprise so that the processing rule is invoked only when you are receiving a 997 functional acknowledgment (and not when sending one).
Document Type	Selected Document Types. Select the document type X12 4010 997 Specify X12 4010 997 as the TN document type for the 997 functional acknowledgment to ensure that the processing rule is only invoked for this acknowledgment 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 Acknowledgments" on page 55.

Creating Services to Process HIPAA Acknowledgments

The HIPAA standard does not mandate how to process acknowledgments. 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 acknowledgments:

- TA1 technical acknowledgment: the wm.estd.hipaa.sample:processHipaaTA1 service.
- 997 functional acknowledgment and other types of acknowledgments: wm.estd.hipaa.sample:processHipaaFA service.

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

An example of the type of processing you might want to perform is updating information in your external system based on the information in the acknowledgment. To do so, you would map data from the HIPAA acknowledgment to the data format required by your external system, and then send the document to that system. For more information about mapping data from HIPAA acknowledgments (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, 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 acknowledgment to the Trading Networks database.

Input Variables

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

Output Variables

None.

Usage Notes

Use this service to receive a HIPAA real-time or batch transaction, a TA1 technical acknowledgment from a trading partner, or acknowledgments such as 997 and 999. 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 acknowledgment.
- application/EDIStream, application/EDI, or application/X12 when sending a HIPAA transaction or 997 functional acknowledgment.

pub.estd.hipaa:recognizeAcknowledgements

This service recognizes and persists an acknowledgment in the Trading Networks database.

Input Variables

Ack String acknowledgment data.

Output Variables

None.

pub.estd.hipaa:recognizeTA1

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

Input Variables

TA1	String Technical acknowledgment data.
prtIgnoreDocument	String Indicates 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 acknowledgments, and formats acknowledgments 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 the appropriate Trading Networks administration guide for your release as noted in the "Document Titles" section of "About This Guide" on page 5.
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` - Default. Do not split the data into separate files.

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 acknowledgments corresponding to each interchange validated.
997	String List List of the functional acknowledgments corresponding to each functional group validated.
999	String List List of the implementation acknowledgments corresponding to each functional group validated. **Note:** This applies to version 5010 only.
277U	String List List of the Unsolicited Claim Acknowledgments generated for 837 transactions. **Note:** This applies to version 4010 only.
277A	String List List of the Claim Acknowledgments 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 acknowledgments 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 email message to the appropriate person (for example, to correct errors). You can also customize these reports to ignore certain validation level messages, display a custom user message, and prevent the generation of certain acknowledgments, by configuring HIPAA TPA parameters. For details, see "Step 5: Create HIPAA Trading Partner Agreements" on page 33.