SYBASE®

User's Guide

Sybase® HIPAA Accelerator

6.0

[Windows]

DOCUMENT ID: DC37002-01-0600-01

LAST REVISED: June 2006

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

About This Book

The Sybase® HIPAA Accelerator is an add-on accelerator to the Sybase® Adapter for EDI, EDI Server, and Adapter Suite for EDI products. When used in conjunction with ECMap, Sybase HIPAA Accelerator allows for rapid development and deployment of HIPAA-compliant EDI messages in accordance with the HIPAA Implementation Guides and Addenda.

Audience

This document is for application engineers and technical consultants who manage Sybase HIPAA Accelerator.

How to use this book

This book describes how to use Sybase HIPAA Accelerator. It is organized into the following chapters:

- Chapter 1, "About Sybase HIPAA Accelerator" briefly describes the Health Insurance Portability and Accountability Act (HIPAA) and details the Sybase HIPAA Accelerator solution.
- Chapter 2, "Working with Compliance Maps" describes how to set up compliance maps, import cross-reference tables from map to map, and run HIPAA X12 data through the maps.
- Chapter 3, "Running and Testing Compliance Maps" describes how to run HIPAA compliance maps and enable optional edits to the maps.
- Chapter 4, "Troubleshooting Map Errors" describes common errors that HIPAA compliance maps might encounter.

Related documents

The following documents ship with Sybase HIPAA Accelerator:

- *Sybase HIPAA Accelerator New Features Guide*
- *Sybase HIPAA Accelerator Installation Guide*
- *Sybase HIPAA Accelerator User's Guide*
- *Release Bulletin for Sybase HIPAA Accelerator*

Additional documents are referred to in the Sybase HIPAA Accelerator documentation to supply you with specific information that supports this product. See:

- *ECMap User's Guide* to understand and build structured information messages

- *ECMap Reference Guide* to understand and recognize informational messages
- *ECRTP Reference Guide* to use the data transformation engine

Documentation that supports Sybase HIPAA Accelerator can be found on the Product Manuals Web site at http://www.sybase.com/support/manuals. Select Sybase HIPAA Accelerator from the drop-down list, and click Go.

Other sources of information

Use the Sybase Getting Started CD, the SyBooks CD, and the Sybase Product Manuals Web site to learn more about your product:

- The Getting Started CD contains release bulletins and installation guides in PDF format and may also contain other documents or updated information not included on the SyBooks CD. It is included with your software. To read or print documents on the Getting Started CD, you need Adobe Acrobat Reader, which you can download at no charge from the Adobe Web site using a link provided on the CD.
- The SyBooks CD contains product manuals and is included with your software. The Eclipse-based SyBooks browser allows you to access the manuals in an easy-to-use, HTML-based format.

  Some documentation may be provided in PDF format, which you can access through the PDF directory on the SyBooks CD. To read or print the PDF files, you need Adobe Acrobat Reader.

  Note Refer to the *SyBooks Installation Guide* on the Getting Started CD, or the *README.txt* file on the SyBooks CD for instructions on installing and starting SyBooks.

- The Sybase Product Manuals Web site is an online version of the SyBooks CD that you can access using a standard Web browser. In addition to product manuals, you will find links to EBFs/Maintenance, Technical Documents, Case Management, Solved Cases, newsgroups, and the Sybase Developer Network.

  To access the Sybase Product Manuals Web site, go to Product Manuals at http://www.sybase.com/support/manuals/.

- Infocenter is an online version of SyBooks that you can view using a standard Web browser. To access the Infocenter Web site, go to Sybooks Online Help at http://infocenter.sybase.com/help/index.jsp.

Sybase certifications on the Web

Technical documentation at the Sybase Web site is updated frequently.

❖ **Finding the latest information on product certifications**

1 Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.

2 Click Certification Report.

3 In the Certification Report filter select a product, platform, and timeframe and then click Go.

4 Click a Certification Report title to display the report.

❖ **Finding the latest information on component certifications**

1 Point your Web browser to Availability and Certification Reports at http://certification.sybase.com/.

2 Either select the product family and product under Search by Product; or select the platform and product under Search by Platform.

3 Select Search to display the availability and certification report for the selection.

❖ **Creating a personalized view of the Sybase Web site (including support pages)**

Set up a MySybase profile. MySybase is a free service that allows you to create a personalized view of Sybase Web pages.

1 Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.

2 Click MySybase and create a MySybase profile.

Sybase EBFs and software maintenance

❖ **Finding the latest information on EBFs and software maintenance**

1 Point your Web browser to the Sybase Support Page at http://www.sybase.com/support.

2 Select EBFs/Maintenance. If prompted, enter your MySybase user name and password.

3 Select a product.

4 Specify a time frame and click Go. A list of EBF/Maintenance releases is displayed.

Padlock icons indicate that you do not have download authorization for certain EBF/Maintenance releases because you are not registered as a Technical Support Contact. If you have not registered, but have valid information provided by your Sybase representative or through your support contract, click Edit Roles to add the "Technical Support Contact" role to your MySybase profile.

5 Click the Info icon to display the EBF/Maintenance report, or click the product description to download the software.

Conventions

This documentation uses the following typographic conventions:

Item	Description
`Code`	SQL and program code is displayed in a monospaced (fixed-width) font.
`User entry`	Text entered by the user is shown in bold serif type.
emphasis	Emphasized words are shown in italic.
file names	File names are shown in italic.
database objects	Names of database objects, such as tables and procedures, are shown in sans serif type in print, and in italic online.
sybase\bin	A backward slash ("\") indicates cross-platform directory information. A forward slash ("/") applies to information specific only to UNIX. Directory names appearing in text display in lowercase unless the system is case sensitive.
File > Save	Menu names and menu items are displayed in plain text. The angle bracket indicates how to navigate menu selections, such as from the File menu to the Save option.
`parse|put|get`	The vertical bar indicates • Options available within code • Delimiter within message examples
segment	Bold text indicates a glossary term.

If you need help

Each Sybase installation that has purchased a support contract has one or more designated people who are authorized to contact Sybase Technical Support. If you cannot resolve a problem using the manuals or online help, please have the designated person contact Sybase Technical Support or the Sybase subsidiary in your area.

CHAPTER 1

About Sybase HIPAA Accelerator

About this chapter

This chapter briefly discusses the HIPAA requirement and describes Sybase HIPAA Accelerator and its components.

Contents

What is HIPAA?

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), a federal law that sets basic requirements that hospitals, physicians, and managed care companies must meet.

The Administrative Simplification provision, a requirement of primary interest to medical practices, contains requirements for the uniform transfer of electronic health care data, such as for billing and payment, protection of patient privacy, and data security.

Standardized formats and data content

For the health care industry to comply with HIPAA and achieve potential administrative cost savings with Electronic Data Interchange (EDI), the Accredited Standards Committee (ASC) X12 developed standards to be implemented consistently by all organizations.

To facilitate uniform implementation, HIPAA's goal is to simplify and encourage the electronic transfer of information by replacing many of the current nationally-used nonstandard formats with a single set of electronic transactions to be used throughout the health care industry.

EDI standards

The X12 format, designed and maintained by the American National Standards Institute (ANSI), provides standard data formats that enable the exchange of business documents between trading partners. Different industries use different data formats or transaction types for different purposes. Common to all, however, is a three-digit numerical designation, which identifies these different transactions; for example, an 834 Benefit Enrollment and Maintenance transaction.

The standard defines a hierarchy of levels—Interchange, Group and Transaction control segments—and specifies both the syntax and semantics of messages. For example, a field designated as quantity might be syntactically specified as required or optional, and the minimum and maximum size of the field might be syntactically defined as well.

HIPAA standards

HIPAA X12 standards are a specific subset of the X12 library of standards. Developed within X12N, the Insurance subcommittee of X12, the HIPAA standards provide a strict and unambiguous interpretation of the various HIPAA transactions named in the Final Rule. This interpretation is presented in a format called an Implementation Guide. HIPAA Implementation Guides, sometimes referred to as IGs, document a specific interpretation of the syntax and semantics of each transaction.

HIPAA Implementation Guides

The HIPAA Implementation Guides satisfy several requirements:

- Comply with HIPAA and its associated rules
- Facilitate a smooth transition to the EDI environment by providing standardized data requirements and content for users of each HIPAA transaction
- Allow the electronic exchange of information from computer to computer without human involvement

The following table lists the transaction standards as implemented through the appropriate Guide Addenda. Computer-based transmissions of the following transaction types must comply with the HIPAA standards.

Transaction	Title and use
270/271	**Health Care Eligibility Benefit Inquiry and Response** Provider uses the 270 to request details of health care eligibility and benefit information or to determine if an information source organization has a particular subscriber or dependent on file. Payer uses the 271 to respond to 270 inquiries.
276/277	**Health Care Claim Status Request and Response** Provider uses to request the status of health care claims. Payer uses to respond to 276 requests.
275	**Additional Information to Support a Health Care Claim or Encounter** Provider uses the 275 to send requested information about a claim or encounter.
277	**Health Care Claim Request for Additional Information** Payer uses the 277 to request additional information about a health care claim or encounter.
278	**Health Care Services Review Information Request and Response** Health care providers use *request* transactions to request information on admission certifications, referrals, service certifications, extended certifications, certification appeals, and other related information. Review entities use *response* transactions to respond to inquiries.

Transaction	Title and use
820	**Payment Order/Remittance Advice** Insurance companies, third-party administrators, payroll service providers, and internal payroll departments use the 820 to transmit premium payment information.
834	**Benefit Enrollment and Maintenance** Benefit plan sponsors and administrators use the 834 to transmit enrollment and benefits information to each other.
835	**Health Care Claim Payment/Advice** Payer and provider use the 835 to make payments on a claim, send Explanation of Benefits (EOB) remittance advice, or to send both the payment and EOB in the same transaction.
837	**Health Care Claim** There are three separate Implementation Guides for 837 Health Care Claims: Dental, Institutional, Professional Each is used by the provider—dentist/dental group, clinic/hospital, and physicians/surgeons—or between payers to submit and transfer claims and encounters to the payer.

Historically, health providers and plans have used many different electronic formats. HIPAA's primary goal is to simplify the complex process of administration and payment of health care claims by implementing a single transaction standard and establishing the code sets used.

Under the enacted regulations, health plans will be able to reimburse providers, authorize services, certify referrals, and coordinate benefits using a standardized electronic format. Additionally, providers will be able to check eligibility for coverage, check claim status, request referrals and service authorizations, and receive electronic remittance to post receivables.

Who is affected by HIPAA requirements?

HIPAA applies to the following health care organizations:

- Health plans
- Health care providers, such as hospitals and physicians, that conduct health transactions electronically
- Health care clearing houses that convert health care data between HIPAA-compliant and non-compliant formats

Entities that pay health care claims, as well as the providers and clearinghouses exchanging electronic payment information with each other, are affected by HIPAA requirements.

Getting additional information about HIPAA

For more detailed information on HIPAA and the Administrative Simplification provision, see the following Web sites:

- Health and Human Services Web site at http://aspe.hhs.gov/admnsimp/index.shtml
- Centers for Medicare and Medicaid Services Web site at http://www.cms.hhs.gov/hipaa/default.asp

Note HIPAA X12 Implementation Guides are available to download from the Washington Publishing Company Web site at http://www.wpc-edi.com.

Sybase HIPAA Accelerator solution and components

Sybase provides the first complete, easily administered health care transaction product. The Sybase HIPAA Accelerator is an add-on accelerator to the Sybase Adapter for EDI, EDI Server, and Adapter Suite for EDI products. When used in conjunction with ECMap, Sybase HIPAA Accelerator allows for rapid development and deployment of HIPAA-compliant EDI messages in accordance with the HIPAA Implementation Guide Addenda.

Whereas it can take health care entities months to create a compliance methodology, Sybase HIPAA Accelerator supplies an immediate solution that includes the following components:

- A standards database containing X12 transactions
- Compliance maps and source map files
- HIPAA-compliant test data
- Support for HCCO CCAP and external code set testing

Standards database

Sybase HIPAA Accelerator's standards database contains the twelve X12 transactions as defined in the HIPAA Implementation Guides. Standards and maps for Sybase HIPAA Accelerator are based on and conform with the October 2003 HIPAA Implementation Guide Addenda.

Each HIPAA standard contains all of the required and situational data segments and elements as specified by the HIPAA Implementation Guides. HIPAA-defined transactions levels, maximum and minimum occurrences, not used elements, and implementation code lists are incorporated into the standards and are easily identifiable.

HIPAA compliance maps

Sybase HIPAA Accelerator distributes maps that facilitate compliance and validate data syntactically and semantically. These maps perform several key functions:

- Verify inbound and outbound HIPAA X12 transactions and check that required and conditional segments and elements are present, where appropriate
- Confirm that only the appropriate code values are present, that minimum and maximum occurrences have not been violated, and that data is not present within not used elements
- Let you add, delete, or change compliance rules, which allows for business logic and flow and validation of information, such as member numbers, provider numbers, and dates of birth versus dates of service

  Note Modifying EDI data is a business-specific decision. Although Sybase HIPAA Accelerator maps impose no restrictions, Sybase strongly recommends business owner approval.

- Capture and report non-compliance errors to a transaction log in ECMap

You can run data through the Sybase HIPAA Accelerator compliance maps with no modifications to verify that your data is HIPAA compliant. Since you also receive source map files, you can alternatively modify the maps by applying your own business rules and specific data checks.

Compliance map error tracking

Errors captured by the Sybase HIPAA Accelerator compliance maps are reported to ECMap's Trans Log. This error logging identifies noncompliant data and lets you build business processes around the event, such as the submission of a 997 functional acknowledgement.

Situations that HIPAA compliance maps trap

The following list represents situations that the HIPAA compliance maps trap:

- Missing mandatory data segment or data element
- Unexpected segment or loop – invalid map flow
- Invalid internal code value
- Data length exceeds maximum or less than minimum
- Maximum use exceeded for segment or loop
- Invalid data format for date or time
- Not used element contains data
- Invalid data type, such as alphanumeric or numeric only
- Violation of reasonable conditional edits (gray box rules)
- Violation of semantics contained in the front matter of the Implementation Guide that can be reasonably quantified

You can also enhance the HIPAA compliance maps to validate external code values, such as ZIP codes, country codes, and the like.

Situations that HIPAA compliance maps do not trap

The HIPAA compliance maps do not trap the following situations:

- Invalid crosswalk, such as application data, subscriber's last name mapped to X12 transaction, or a subscriber's first name
- Conditional edits that cannot be reasonably verified, such as if the presence of a person's middle name is required, if known. It would be unreasonable to determine whether the submitting trading partner knew the patient's middle name.

Error trapping gives you enough information to either modify the EDI data to create valid compliance information or notify senders so they can quickly correct the data. See Chapter 4, "Troubleshooting Map Errors" for more information.

Compliance map rules development guidelines

Sybase used the following guidelines in developing the compliance rules supplied with Sybase HIPAA Accelerator 6.0:

- The maps are based on the final Implementation Guide Addenda. Sybase does not create product based on drafts or HIPAA documents that are not finalized.

- If a gray box rule, note, or front matter explanation exists within the published HIPAA Implementation Guides and a validation rule can be reasonably determined, the gray box rule, note or front-matter explanation is included in the compliance maps.
- Assumptions or leaps of logic were not employed in the creation of validation rules.
- "Should" is interpreted as optional, whereas "must" is interpreted as required.
- Assumptions regarding negative conditions are not included. For example, if a gray box rule states, "If it is Tuesday, the patient's eye color is required," the rule would be written to verify the day of the week. If the day of the week was Tuesday, the compliance map would require that "eye color" be included. However, if the day of the week was any day but Tuesday and the "eye color" was still present, a rule would not be written to reject that condition.

Sybase HIPAA Accelerator testing

This section describes Sybase HIPAA Accelerator support for HCCO CCAP and external code set testing.

Support for HCCO CCAP testing

The HIPAA Conformance Certification Organization (HCCO) is a nonprofit organization that provides the health care industry with guidelines for complying with HIPAA regulation through the use of accreditation and certification standards and services. HCCO brings interoperability of HIPAA transactions to health care through its CCAP testing programs by helping vendors in interpreting the Implementation Guides in the same manner. CCAP is the only process available to vendors to test interoperability across health care covered entities.

Sybase HIPAA Accelerator implementation adheres to a careful interpretation of the gray box rules, called Industry Notes in the HIPAA Implementation Guides. Because these rules are subject to different interpretations, Sybase is involved with HCCO CCAP.

For more information on Sybase support for HCCO CCAP test suites, see "Support for HCCO CCAP testing" on page 48. See also the HIPAA Conformance Certification Organization Web site at http://www.hcco.us/.

Support for code set testing

The Strategic National Implementation Process (SNIP) is a WEDI-sponsored program that helps health care communities identify and resolve HIPAA implementation issues. WEDI, the Workgroup for Electronic Data Interchange, is a health care industry group that lobbied for HIPAA Administrative Simplification and has a formal consultative role under the HIPAA legislation. See Table 1-1 for the WEDI/SNIP testing types that Sybase HIPAA Accelerator 6.0 supports.

Table 1-1: WEDI/SNIP testing types supported by Sybase HIPAA Accelerator

Testing type	Description
Type 1: EDI syntax integrity testing	Validates basic syntactical integrity of EDI submission: segments, order, element attributes, testing numeric values in data elements, validation of X12 syntax, and compliance with X12 rules.
Type 2: HIPAA syntactical requirement testing	Testing for HIPAA IG-specific syntax requirements, such as limits on repeat counts, used/not used qualifiers, codes, elements and segments. Also, testing for HIPAA required or intra-segment situational data elements, testing for nonmedical code sets, and values and codes noted in the IG via an X12 code list or table.
Type 3: Balancing	Testing the transaction for balanced field totals, financial balancing of claims or remittance advice, and balancing of summary fields. For example, all claim line item amounts equal the total claim amount.
Type 4: Situation testing	Testing of specific inter-segment situations described in the IG, such that: If A occurs then B must be populated. This is considered to include the validation of situational fields given values or situations present elsewhere in the file. Example: if the claim is for an accident, the accident date must be present.
Type 5: External code set testing	Testing for valid IG-specific code set values and other code sets adopted as HIPAA standards. This level of testing validates the code sets and ensures the usage is appropriate for any particular transaction and appropriate with the coding guidelines that apply to the specific code set. Validates external code sets and tables, status codes, adjustment reason codes, and their appropriate use for the transaction. *Sybase HIPAA Accelerator supports type 5 validation for some situations. For example, Sybase HIPAA Accelerator does not support validation of U.S. zip codes.* *Sybase supports medical external code sets.*

Table 1-2: WEDI/SNIP testing types not supported by Sybase HIPAA Accelerator

Testing type	Description
Type 6: Product types or line of services	Testing type is required to ensure that the segments/records of data that differ based on certain health care services are properly created and processed into claims data formats. These specific requirements are described in the IGs for different product types or lines of service. For example, ambulance, chiropractic, podiatry, home health, parenteral and enteral nutrition, durable medical equipment (DME), psychiatry, and other specialized services have specific requirements in the IG that must be tested before putting the transaction in production. *This type of testing applies only to a trading partner candidate that conducts transactions for the specific line of business or product type*.
Type 7: Implementation Guide-specific trading partners	The IGs contain some HIPAA requirements that are specific to Medicare, Medicaid, and Indian Health. Compliance or testing with these payer-specific requirements is not required from all trading partners. If the trading partner candidate intends to exchange transactions with one of these IG special payers, Type 7 testing is required. When a certification service certifies a trading partner for compliance, the certification service must indicate whether these payer-specific requirements were met during the certification process. Other payers and trading partners may have their own specific business requirements. Unless, however, they are listed in the HIPAA IGs, they are not HIPAA requirements. These non-HIPAA trading partner specific requirements must be tested as part of the business-to-business testing.

For additional information, see the Workgroup for Electronic Data Interchange Web site at http://www.wedi.org/.

CHAPTER 2

Working with Compliance Maps

About this chapter

This chapter describes how to upgrade your version of Sybase HIPAA Accelerator, set up compliance maps, and import cross-reference tables from map to map.

Sybase HIPAA Accelerator supports two setup types for running HIPAA X12 data through a compliance map: default compliance maps and compliance maps with business rules.

For complete details on window entries, menu choices, and other advanced setup options, refer to the *ECMap User's Guide*. For a comprehensive list of informational messages, see the *ECMap Reference Guide*.

Contents

Setting up compliance maps using ECMap

This section provides a brief overview of ECMap functionality and describes how to set up the HIPAA compliance projects and maps using ECMap, a powerful mapping tool that provides support for creating and processing structured information messages. For advanced setup options, refer to the *ECMap User's Guide*.

Format classes that ECMap supports

ECMap can handle three classes of formats:

- Traditional formats of flat files and databases
- EDI Standards: X12, EDIFACT, NCPDP, and HL7
- HTML or XML data

You can also import other standards with the EDI Standard Exchange Format (SEF) Import utility. Once imported, you can use these standards like the other standards that are bundled with the product. ECMap lets you perform application-to-application integration as well as Web-enabling XML data and XML-enabling databases.

Types of maps you can create with ECMap

ECMap lets you create the following:

- Transaction maps that perform data conversions between application data and EDI standards
- Any-to-any maps that convert data directly from one application to another
- Any-to-any maps that perform data conversions between HTML/XML data and application data
- Any-to-any maps that perform data conversions between HTML or XML data and EDI standards.

What ECMap does

ECMap has the ability to

- Automatically generate a set of record and field definitions from a COBOL copybook, an ODBC file, a map, or a special file
- Automatically generate an ODBC database table from a set of record and field definitions
- Use a wide variety of rule commands, including conditional logic, to imbed business rules and proprietary compliance checks in your map
- Use a wide range of SQL commands from within a SQL rule command, allowing direct integration with any ODBC-compliant database
- Access functions outside of the product through User Exit rule commands

- Perform dynamic map switching at runtime
- Perform interactive, real-time transactions
- Perform any-to-any mapping, directly integrating diverse application databases
- Process large volumes at high speeds, without having to break up and reassemble the data
- Translate data independent of file size
- Perform data conversions between HTML or XML data and EDI standards
- Automatically generate a set of record and field definitions from an HTML form
- Automatically create the template for an HTML form from a set of record and field definitions
- Dynamically build and populate an HTML form based on retrieved data and an HTML form template
- Perform dynamic interactions between an HTML form and the values in a database
- Map XML data to a proprietary application
- Import customized standards—such as those based on Implementation Guides—and use them just as you use the major standards included with the tool, X12, EDIFACT, and HL7
- Automatically create a field from an EDI element during map development
- Perform conditional mapping, by associating particular mapping commands to a specific trading partner, to the presence or absence of data and the like
- Quickly and easily perform element-to-field mapping for any standard supported by ECMap
- Map directly from one proprietary application to another
- Create and run special compliance maps to verify that the data a map processes is compliant with the standard used
- Automatically generate a batch file that includes all of the switches needed to run the map from a command line

- Use the runtime capability of substituting either a new input file or a new output file for the file specified in the map, regardless of whether the files are flat files or ODBC databases
- Pass parameters into the map at runtime
- Verify compliance with the HIPAA mandate

Creating a project

ECMap uses projects to organize maps so they are easy to locate and use. You can set up projects in any way that suits your business purposes, such as creating projects based on trading partners or on business applications.

You can add, modify, select and delete projects, as well as import or export an entire project with all of its associated maps.

Where data is stored

Each time you create a project, the system adds the data to a Microsoft® Access database file called *projects.mdb*. This master file comprises three tables, mproject, mtable, and mxref, which contain information about all of the projects, maps, and cross-reference tables in ECMap. The information in these tables is updated each time that you add, modify, or delete a project, map, or cross-reference table.

mproject table

The mproject table contains the names of all of the projects in your system. It contains all of the information entered in the five text boxes within the New Project window:

- Project Name
- Project Description
- Project Directory
- Contact
- Phone Number

mtable table

mtable contains the names of all of the projects and maps in your system. The project name links this table to the mproject table, and the project name/map name combination links this table to the mxref table. Each record in the table contains the name of a project, a map within that project, and the related trading partner information. The mtable table contains all of the information you entered in the four tabs of the Map Definition window.

mxref table

The mxref table contains the names of all the project, maps, and cross-reference tables in your system. Each record in the table contains the name of a project, a map within that project, and a cross-reference table used in that map. The project name links this table to the mproject table, and the project name/map name combination links this table to the mtable table. Since the same cross-reference tables can be used in more than one map, there may be multiple records that have the same cross-reference table name.

When you export a project, ECMap creates a copy of these same three tables, but they contain information only for the project being exported. When you import the project, ECMap uses the exported project-specific information in these three tables to update the master *projects.mdb* database in the ECMap installation to which the project is being imported.

❖ **Starting ECMap**

1 Double-click the ECMap icon on your desktop or select Start > Programs > Sybase > ECMap > ECMap.

2 When the Login window displays, accept the default user name, `Admin`.

3 Type the password, `ecmap`, and click OK.

Note The password is case sensitive. Use lowercase.

❖ **Creating a project**

1 In the ECMap main window select File > Project > New. The New Project window displays.

2 Type information into the text boxes in the Project group:

a Project Name – Type a short title that helps you quickly recognize the contents of the project. This field is required.

b Project Description – Type a brief explanation of the project. This field is optional.

c Directory – Click Browse to navigate to the folder or directory where the project is physically stored and double-click the folder to populate the field. This field is required.

d Contact – Type the name of the individual responsible for the maps in this project. This field is optional.

e Phone Number – Type the telephone number of the individual responsible for the maps in this project. This field is optional.

3 Click OK to return to the Project window.

4 Highlight the Project you just created, right-click and choose Select from the submenu.

The project name now displays in ECMap's status bar in the main window.

Creating default compliance maps

A map is a set of instructions used to transform data from one format to another. ECMap can create the following maps:

- *Transaction maps* use EDI standards data in the mapping process, either as input or output.
- *Any-to-any maps* use application data as both the input and the output. An any-to-any map can use EDI data, but it treats the EDI data as application data, rather than standards data.

You can add, select, modify, copy, or delete maps. You can also generate all maps in one project, generate all maps in all projects, or view all maps in a project.

Map direction

Transaction maps are said to be either inbound or outbound.

- An *inbound map* uses an EDI message to create application data. The EDI message is the input to the map, and it is being sent in to your company from your trading partner.

  ECMap also uses two specialized inbound maps, compliance maps and print maps. See the *ECMap User's Guide* for more information on these two maps.

- An *outbound map* uses application data to create an EDI message. The EDI message is the output of the map, and it is generally being sent from your company out to your trading partner.

In ECMap, each transaction map is associated with a specific EDI standard—X12, EDIFACT, NCPDP, or HL7—and a specific transaction within that standard.You assign a map type when you create a new map.

Where maps are stored

Maps are stored in projects. You must have a separate map for each business message that you exchange with a trading partner. For EDI transactions, this means one map per message type, application system, and map direction. The name given to a map often reflects the message type and the direction. For example, an X12 map that uses your company's internal application data to produce an EDI invoice that is sent to a trading partner might be named 810OUT.

❖ **Accessing the Map window**

You perform all map-related actions from the Map window.

- Click the Map icon on the main ECMap toolbar or Choose File > Map > Select from the main menu.

Creating a map

Use the following procedure to create a default compliance map.

❖ **Creating a map**

1 Right-click the project you just created and select New > Map from the submenu.

The New Map Definition window displays with three tabs: Map Properties, Map Directories, and Map DSN. The Map Properties tab is initially active. You type information into various fields.

2 Populate the fields in the Map group:

a In the Project text box, the program automatically populates the field from the current project.

b In the Map Name field, type a map name; for example, *HIPAA_270_4010_60*. This field is required.

See the *Sybase HIPAA Accelerator Installation Guide* for a list of map names provided in the Sybase HIPAA Accelerator installation.

c In the Map Type field, click the arrow and choose X12. This field is required and activates the Options group.

3 In the Options group, populate the following fields:

a In the Transaction field, type the transaction set number. This field is required.

This is the HIPAA transaction set corresponding to the HIPAA map name you entered above. Possible choices are 270, 271, 276, 277, 278, 820, 834, 835 and 837.

b In the Direction field, click the arrow and choose IN.

Note The direction of a compliance map must be IN, whether the data you are testing is inbound or outbound.

c In the Version field, click the down arrow and choose 004010.This field is required.

d In the Description field, type a brief description. This field is optional.

e In the Century Minimum field, type a value. This field is required.

f Select Y for 8 Digit Date in X12 Envelope.

4 Click the Map Directories tab to make it active and populate the fields within.

ECMap uses the directory location specified on the New Project window followed by the map name specified to automatically populate all directories except for the EDI Standard Tables. In the following example, the directory specified in the New Project window was *C:\maps\MyMaps* and the map name was *HIPAA_270_4010_60*.

When you define your EDI Standard Tables location on the New Map Definition window, refer to the location of the HIPAA standards.

Warning! It is very important that you point to the directory with the Sybase HIPAA Accelerator standards and not the default ECMap standards.

a Click Invert to protect the paths of all of the supplied map information, or click Protect/Change for a specific directory to toggle back to protect or change a directory.

b Click Change All to type the path of the EDI Standard Tables. A dialog box opens for you to select a directory.

c Select the directory path to the HIPAA standards.

If you used the default install directory, identify the path as *\Program Files\Sybase\HIPAA52\ Standards\<Standard>*. If you chose a different directory path during installation, you must use that directory path.

5 Click the Map DSN tab if the trading partner and log information are stored in databases that will be accessed through ODBC.

a In the Trade Partner group, click the Data Source Name arrow. The Data Source Names window displays.

b Double-click a Data Source Name from the list to automatically populate the fields in the Trade Partner group.

If you have not created the DSN, click Configure Data Source to open the ODBC configuration window. Once you have created your DSN or DSNs, you may proceed.

Note For certain databases, such as Microsoft® SQL Server and Oracle, you may need to edit the string in the text box manually to add a user ID and password.

c To test the connections, click Test Trade Partner Connection in the Trade Partner group or Test Log File Connection in the Log group.

If you select Clear TP Fields, the program removes all of the information you inserted in the text boxes on the Trade Partner section of this tab. If you select Clear Log Fields, the program removes all of the information you inserted in the text boxes on the Log section.

6 Click OK to return to the Project window.

Modifying the ALL TradePartner

ECMap uses mailboxes for routing. Mailbox folders are directories where the runtime engine (ECRTP) drops off EDI data produced by outbound maps and compliance runs and places inbound EDI data being passed through.

Mailboxes are attached to the trading partner and are used for both inbound and outbound routing.

- GOOD mailboxes are used by compliance maps.
- BAD mailboxes are used by compliance maps and inbound maps.
- IN mailboxes are used both by inbound maps and by outbound maps with the Route In switch set.
- OUT mailboxes are used both by outbound maps and by inbound maps with the Route Out switch set.
- OTHER mailboxes are used internally for data that moves between IN or GOOD folders into the OTHER folder for processing.

When you define a mailbox the folders, GOOD, BAD, IN, OUT AND OTHER appear in the directory in which the mailbox (file) is located. This directory is determined by the entry you made on the Trading Partner or Trade Agreement window in ECMap.

The transaction—all of the data between the ST and SE elements—that contains noncompliant (bad) data produced by compliance maps is placed in the BAD directory of the ALL TradePartner mailbox. For this to happen, the ALL TradePartner must have a mailbox.

Note The following procedure uses the ALL TradePartner mailbox, but you can also assign mailboxes to individual trading partner file entries.

For more detailed information on mailboxes, see *ECMap User's Guide*.

❖ **Modifying the ALL TradePartner**

A mailbox is another name for a directory where map-produced EDI data resides. ECMap and EC Gateway use five mailboxes (files):

1 In ECMap's main window, select File > Address Book > Contacts (Trading Partner). The Trading Partners window displays.

2 Right-click the ALL TradePartner and choose Properties from the submenu. The Trading Partner – Properties window displays.

3 Click the General tab to make it active.

4 In the Trading Partner group, click Browse to the right of the MailBox Folder field and locate the path to a mailbox for the ALL TradePartner.

5 Click OK to populate the field with the path to the mailbox directory.

6 Click OK to return to the Trading Partners window.

Changing the map's purpose and status

This section describes two procedures: changing the purpose of the map to CMP (compliance) and confirming that the status corresponds to the status on ISA 15 of the incoming EDI data.

❖ **Changing the map's purpose**

1 In the Trade Agreements With Trade Partner: ALL window, select Edit > Properties. The Standard Type for Map window displays.

2 Click to select one of the standard types and click OK.

The Trade Agreement - Properties window displays with tabs enabled: General, Overrides, and X12, EDIFACT, or HL7, depending on which standard type you selected. The General tab is active initially.

3 In the Map Information group, click the Map Type arrow and choose CMP.

❖ **Confirming the map's status**

1 In the Map Information group, click the Test Indicator arrow. It should be the same as the status indicated in ISA 15 on your incoming EDI data: T (Test) or P (Production).

2 In the Version/Release/Industry Identifier Code field, type the version suffix identified in the HIPAA Implementation Guide for your specific transaction; for example, 270 has a version suffix of X092. Type this information after the default of 004010, which is the same version you entered on the Map Properties tab.

3 Set the functional acknowledgement, if appropriate.

a If you require no functional acknowledgement, click OK.

b If you require a functional acknowledgement, click the standard type tab that is enabled; for example, X12, EDIFACT, or HL.

1 In the Envelope Information group, click the ISA arrow and choose 00401.

2 In the Notification group, select the Expect FA 997 Functional Acknowledgement check box.

4 Click OK.

For more detailed instructions on building functional acknowledgements, see the *ECMap User's Guide*.

Identifying company information

If you have not already identified your company information, it is necessary to do so before running the map. The company information is the electronic signature for your outgoing EDI messages.

❖ **Identifying company information**

1 In ECMap's main window, select File > Address Book > Signature (Company ID). The Company ID window displays.

2 In the Company ID window, select File > New. The Company ID - New window displays.

3 Identify the Company information:

   a In the Profile Number text box, type a value for the company.

   b In the Name text box, type the company name.

4 Identify the Interchange, which is required.

   The Group, Authorization and Security codes are optional, as described in *ECMap User's Guide* and *ECMap Reference Guide*.

5 Click OK to save the company information.

Creating compliance maps with business rules

When you add rules to a compliance map, first copy the compliance map to an alternate location to retain the original map's integrity. Once you add your business rules to the expanded map and regenerate it, your edited map is ready for use with the associated trading partners.

This section describes copying the map and modifying it with your own business logic.

Refer to the *ECMap User's Guide* for detailed information on window entries, menu choices, and the detailed map modification process.

About rules

Although ECMap lets customers create rules with any rule number, Sybase allocates a range of numbers for customer use: 25000 to 32767. Confining customer-specific logic to a range lets customers easily identify which rules Sybase created and which rules they created.

Note Although the program allows you to create rules using numbers under 25000, there is no guarantee that Sybase will not overwrite the rule number on a subsequent release. To preserve the rules you create, use the Sybase-supplied range.

❖ **Copying a map**

1 In ECMap's main menu, select Utilities > Copy Map. The Copy Map window displays.

   On the Copy Map window, the program populates the Map Name and Project Name text boxes with the names of the currently selected map and the project in which it is stored.

2 You can accept the project and map names entered by the program, or you can change them.

   a To accept the current settings, click Run.

   b To change the project and its associated map, do the following:

      1 Click the Project Name arrow. The Select Project and Map window displays.

      2 Double-click the appropriate project and its associated map. The Select Project and Map window closes and populates the Project Name and Map Name text boxes in the Copy Map window.

3 In the Trade Partner Option group, choose one of the following:

   a Click Include Trade Partner Tables to copy all map-related files and databases, including trading partner tables (tp, tradstat, and wixset).

   b Click Exclude Trade Partner Tables to copy map-related files and databases, excluding trading partner tables.

   You usually *include* the trading partner tables when you copy a map, but you may want to exclude them for various reasons. For example, if you are copying a map to use in a different project, that project might use an entirely different set of trading partner tables.

4 Choose the appropriate option in the Map Copy Direction group. Additional text boxes let you specify where you want the copy to reside.

Choose this option	To do this
This Map to Map	Copy the properties of this map to another map. In the Copy Map To group, click the Browse button next to the Map Name box, choose the appropriate Project Name and Map Name from the dialog box.
This Map from Map	Move the properties of another map into this map. In the Copy Map From group, click the Browse button next to the Map Name box, choose the appropriate Project Name and Map Name from the dialog box.
This Map to Directory	Copy this map to a new directory. In the Copy Map To box, click the Browse button, then choose the destination directory.

Choose this option	To do this
This Map from Directory	Moves the properties of a map in another directory into this map. In the Copy Map From box, click the browse button, then choose the directory where the map resides. If you want to define a new map based on the copy, click Create This Map Definition from Directory Copy.

❖ **Confirming the copy command**

Now that you have set all the options, you are ready to create the copy of your map.

1 Click Run. The program displays a confirmation dialog box that restates the details of the copy map option you have chosen.

2 The program asks for your confirmation before the map is actually copied.

a If you do not want to proceed or you want to change something, click No to return to the Copy Map window.

b If you want to copy the map, click Yes. The map is copied and you return to the main ECMap window.

❖ **Viewing the copy map log**

1 If you want to see a listing of the actions that took place during the copy process, click View Log. The View Log window displays.

2 The information on this window lists each of the databases that were copied. If any problems were encountered, it issues warnings and errors. You should look at all warnings, but they do not necessarily prevent the copied map from running correctly. You must look at errors since they indicate a condition that would prevent the map from running.

❖ **Modifying and regenerating the map**

Make you sure you are working in a copy of the map and not the original when adding additional business edits to the compliance map.

1 Modify your map to add additional logic or data validation that reflects your particular business environment.

When you regenerate and run your modified compliance map, ECMap not only checks for HIPAA compliance but performs the added data checks. Refer to the *ECMap User's Guide* for instructions on modifying your map, using features such as conditional logic, cross-reference tables, and rules.

2 Select Utilities > Generate Compliance Map. The Generate Compliance Map window displays.

3 Click Generate Error for Ignored Elements with Data.

4 Click Run.

5 Click No on the Generate dialog box so that your changes are included in the map file.

❖ **Associating cross-reference tables with maps**

If errors occur during the generation of the map that indicate that cross-reference tables do not exist, you need to associate the tables with the compliance map elements.

1 In ECMap's main window, select Tools > Cross Reference Tables. The Cross Reference Tables window displays a list of all currently used cross-reference tables.

2 Select Files > Directory Scan from the menu.

Any cross-reference tables that are not used in the map are displayed in the Cross Reference Directory Tables window.

3 Select all the tables in the Cross Reference Directory Tables window and click OK.

The tables are added to the list in the Cross Reference Tables window.

4 Regenerate the map.

Upgrading Sybase HIPAA Accelerator

This section contains recommendations on how best to use these features to facilitate upgrading HIPAA compliance maps from one release to the next.

To let customers modify compliance maps to meet their specific business requirements, Sybase HIPAA Accelerator includes compliance maps with source code. Previously, when you upgraded your version of Sybase HIPAA Accelerator, you had to merge your business-specific edits into the new map or maps manually.

This section describes development conventions for Sybase HIPAA Accelerator administrators who modify compliance maps.

When upgrading maps, there are three cases that Sybase HIPAA Accelerator administrators may need to address: Adding to a rule, replacing or deleting a rule, and deleting a command. The following procedures describe these cases.

❖ **Adding to a rule or command**

1 Select the rule and the location within the rule where the additional logic is required.

2 At the selected location, insert a Perform Rule command or an IF …THEN command that calls a new rule from the customer-reserved region, which contains the new logic.

❖ **Replacing or deleting rules**

1 Write the new replacement rule in the customer-reserved region.

2 Modify every Perform Rule command in the map that calls the rule to be replaced to call the new rule instead.

❖ **Deleting commands**

1 Identify the command that needs to be deleted.

2 Depending on which EDI version you are running, perform one of the following steps:

a Disable the command if you are working with EDI 4.x

b Delete the command if you are working with EDI 2.9

In each case, carefully document all modifications as well as the locations of the modifications. This includes, as stated previously, new rules or commands and deleted rules or commands. When merging the changes from one version of Sybase HIPAA Accelerator to the next, refer to your documentation.

For more detailed information on working with rules, see the *ECMap User's Guide*.

Updating maps, rules, and cross-reference tables

Sybase HIPAA Accelerator 6.0 provides two capabilities to facilitate the upgrade process: An import rule capability helps you easily update maps and import rules, and an import XREF utility let you import cross-reference tables from one map to another.

In addition to updating rules, you can modify cross-reference tables. For example, you can add tables to maps to handle certain situations or add values to a table supplied in the compliance map, such as inpatient/outpatient edits in the 837 Institutional map. See "Validating maps against National Employer ID values" on page 40.

Sybase HIPAA Accelerator 6.0 supplies a cross-reference utility that facilitates importing tables from one map to another.

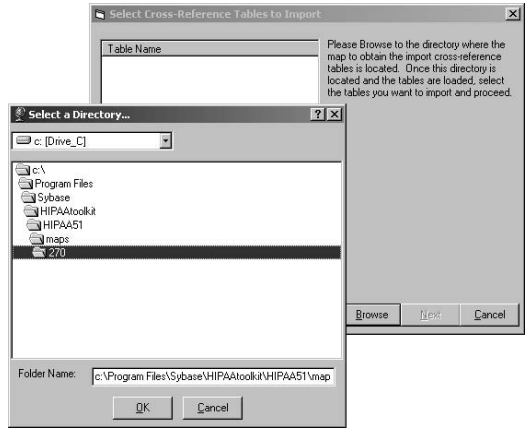
❖ Importing cross-reference tables from one map to another

ECMap must be installed on the machine where you use the cross-reference utility, which works with any version of ECMap.

1 Navigate to the *\Tools* folder in your Sybase HIPAA Accelerator install directory; for example, *C:\Program Files\Sybase\HIPAA52\Tools*, and double-click *XrefImport.exe* to launch the application.

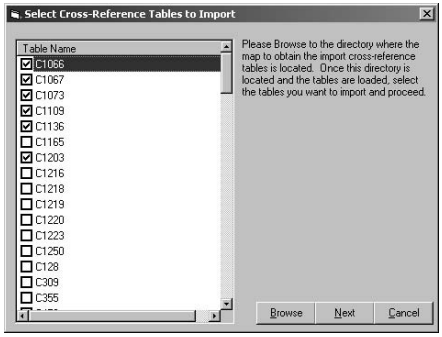
2 Select the location of the source cross-reference tables by browsing to the directory where the map resides (where the tables will be imported *from*). For example, if you are upgrading from Sybase HIPAA Accelerator 5.0.x to 5.1, your source is the location of the version 5.0.x map.

You select one map at a time.



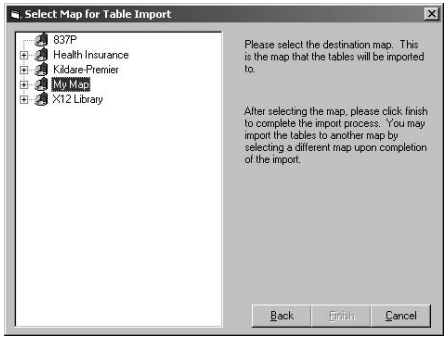
3 Double-click the directory and a list of cross-reference tables defined for that map displays.

4 Check the tables you want to import and click Next.



The Select Map for Table Import screen opens and displays a list of your projects and maps.

5 Open a project and select your destination map (where the tables will be imported *to*). In the case of the upgrade mentioned in step 2, the map you select is the 6.0 version of the Sybase HIPAA Accelerator map.



6 Click Finish to import the tables. The import process runs.

7 If the import table already exists in the destination map, a prompt displays asking if the import table should overwrite the current table. Click Yes to overwrite.

8 When the window opens that indicates the process is complete, click OK to continue.

What to do next

You can begin working with your new map, or you can do one of the following:

- Import the current set of tables to another map by selecting that map on the Select Map for Table Import screen.
- Select a new set of tables from the Select Cross-Reference Tables to Import window and return to the Select Map for Table Import Window.
- Select a different source and import those tables following the same steps.

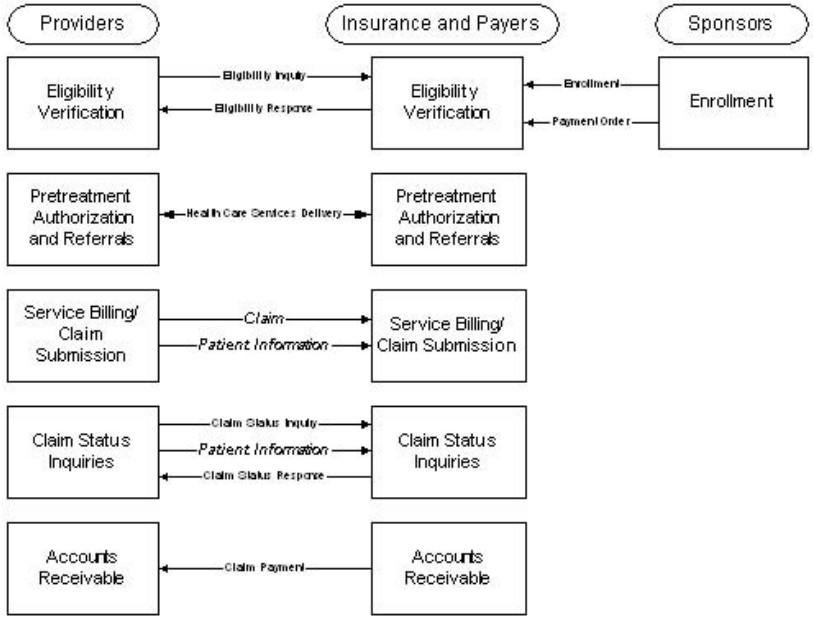
If you import a table to a map and the table did not exist previously, update the map to use the new table by linking it to the appropriate element or rule.

Note ECMap users can also access the cross-reference feature through the ECMap Utilities menu. See the *ECMap User's Guide* for details.

Understanding claims attachments

The Health Insurance Portability and Accountability Act (HIPAA) recently introduced claims attachments into the group of HIPAA transactions. These transactions are based on the X12 version 4050, rather than the 4010 version.

A health care claim attachment conveys supplemental information about the services provided to a specific individual to support evaluation of a claim before it is paid.



Claims attachment usage and goals

The goal of health care claims attachments is to make the process of submitting and adjudicating health care claims more effective and efficient by providing a structured and standard means of requesting clinical/supporting data for health care claims or encounters. Claims attachment usage includes:

- Supporting health care claims adjudication
- Assessing prior authorization
- Validating policies and meet standards
- Providing post-payment review
- Mitigating fraud and abuse

Contributions to the ultimate outreach recommendations included determining the most frequently used attachments; considering the attachments where HL7 messages already existed or were in development; a need to standardize the questions payers ask; and the use of LOINC codes.

What is LOINC?

LOINC stands for Logical Observation Identifier Names and Codes and comprises universal names and ID codes for identifying laboratory and clinical test results and other information meaningful in claims attachments.

LOINC is freeware owned by Regenstrief Institute at http://www.regenstrief.org/ and the Logical Observation Identifier Names and Codes (LOINC) Committee.

Using LOINC allows for specific questions to be asked, when required, as many of the codes required for claims attachments are already present.

Figure 2-1 illustrates the business flow solicited model for claims attachments.

Figure 2-1: Business flow solicited model

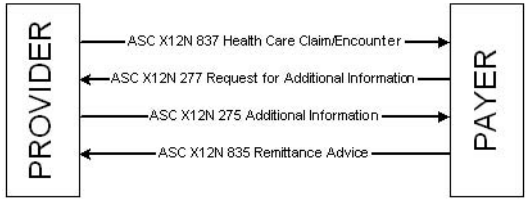
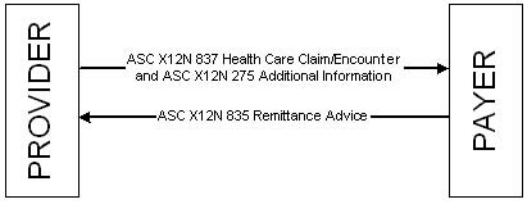


Figure 2-2 illustrates the business flow unsolicited model for claims attachments.

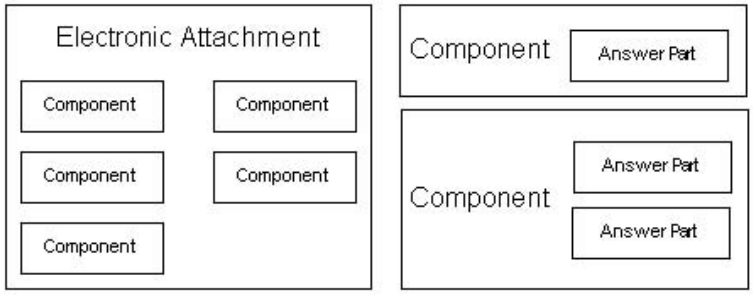
Figure 2-2: Business flow unsolicited model



Structure of claims attachments

As illustrated in Figure 2-3, a 277 asks for attachments or components by sending LOINC, whereas a 275 sends components consisting of answer parts identified by LOINC.

Figure 2-3: Structure of claims attachments



Sybase HIPAA Accelerator 6.0 includes the new claims attachments, along with rules spreadsheets, which document the changes to the compliance maps.

These spreadsheets document the Implementation Guide (IG) map rules and conditions and enable users to quickly find the edits for a particular IG requirement.

HIPAA unique identifiers

HIPAA requires the use of unique identifier numbers for use in health care for individuals, employers, health plans, and health care providers.

The following list represents the status of those identifiers:

- National Provider Identifier: All numeric and 10 positions in length: the first 9 positions are the identifier and the last position is a check digit, which helps detect invalid NPIs. This string of digits may be prefaced by the value ‘80840,’ which is the card issuer ID.
- Employer Identification Number: Federal Employer Identification Number (EIN), 9 digits separated by a hyphen (XX-XXXXXXX). The hyphen is allowed in the third position only; thus the EIN is two digits, hyphen, 7 digits.
- National Health Plan Identifier: No proposed standard.
- National Individual Identifier: No proposed standard (on hold as of the publication of this guide).

Sybase HIPAA Accelerator provides support for the National Provider Identifier and Employer Identification Number data elements.

National Provider Identifier

The purpose of the National Provider Identifier (NPI) is to uniquely identify a health care provider in standard transactions, such as health care claims. NPIs can also be used to identify health care providers on prescriptions, in internal files to link proprietary provider identification numbers and other information, in coordination of benefits between health plans, in patient medical record systems, in program integrity files, and in other ways.

HIPAA requires that covered entities (health plans, health care clearinghouses, and those health care providers who transmit any health information in electronic form in connection with a transaction for which the Secretary of Health and Human Services has adopted a standard) use NPIs in standard transactions by the compliance dates, after which time the NPI will be the only health care provider identifier allowed for identification purposes in standard transactions by covered entities.

The NPI is all numeric and is 10 positions in length: the first 9 positions are the identifier, and the last position is a check digit, which helps detect invalid NPIs.

NPI data element

The NPI data element and its use are described in *Final Rule for the Standard Unique Health Identifier for Health Care Providers (69 FR 3434)*. Usage of the NPI data element in electronic transactions covered under the HIPAA ruling is required as of January 1, 2006.

This section describes the support provided in Sybase HIPAA Accelerator maps, specifically the locations of the NPI data element in the HIPAA transaction maps.

Map rules have been added to the Sybase HIPAA Accelerator maps to test for NPI elements as defined in the HIPAA Implementation Guides (IGs). When an element is found that should contain an NPI value, that element is copied to a string and passed to the NPI test rules.

NPI testing is disabled as delivered in the product. Enable testing by setting Parameter 9 to 'Y' in ECMAP. See the *ECMAP User's Guide* for details on setting parameters.

Table 2-1 illustrates the National Provider Identifier data elements.

Note There are no NPI data elements in the 820 compliance map

Table 2-1: NPI data elements

Compliance map	Loop	HIPAA IG page
270	2100A	46
	2100B	52
	2100B	55
	2100B	65
	2100C	80 - 82
	2100D	121
271	2100A	165
	2100B	179
	2100B	183
	2120C	251
	2120C	261-263
	2120D	329
	2120D	340
276	2100B	63
	2100C	68
277	2100B	143
	2100C	148
278RQ	2010A	71
	2010B	75
	2010E	154
278RP	2010A	267
	2010B	277
	2010CB	325
	2010DB	377
	2010E	389
	2010F	482
834	2310	141-143
835	1000B	73
	2000	80
	2100	113
	2110	157
837D	2010AA	76
	2010AB	86
	2310A	182
	2310B	189
	2310C	195

Compliance map	Loop	HIPAA IG page
	2310D	201
	2420A	291
	2420C	303
837I	2010AA	77
	2010AB	92
	2310A	330
	2310B	337
	2310C	342
	2310E	346
	2420A	466
	2420B	470
	2420C	476
837P	2010AA	83
	2010AB	97
	2310A	271
	2310B	278
	2310C	284
	2310D	290
	2310E	298
	2420A	488
	2420B	494
	2420C	499
	2420D	508
	2420E	513
	2420F	524
275 *4050*	1000C	51
277 RQ for additional info	2100B	58
	2100C	62

Employer Identification Number

In 1998 the IRS agreed to the use of the Employer Identifier Number (EIN) as the identifying number for employers in electronic health care transactions under HIPAA.

The Employer Identification Number is defined as a character string of the following form: XX-XXXXXXX where each X is a digit character from 0 to 9 inclusive. Position 3 in the EIN field is the hyphen character. The EIN processing rules perform validation based on this definition.

The EIN is a data element required by the federal HIPAA legislation; its use is described in the *Federal Register / Vol. 63, No. 115 / Tuesday, June 16, 1998*. This section describes the EIN and its use in the health care system, as well as the functionality added to the Sybase HIPAA Accelerator maps.

A standard employer identifier is needed for electronic health transactions for several reasons:

- Employers, as sponsors of health insurance for their employees, often need to be identified in health care transactions, and a standard identifier for employers is beneficial for transactions exchanged electronically.
- Health care providers may need to identify the employer of the participant on claims submitted to health plans electronically.
- Employers need to identify themselves in electronic transactions when they enroll or unenroll employees in a health plan or make premium payments to health plans on behalf of their employees.
- Employers and health care providers may need to identify an employer as the source or receiver of information about a participant's eligibility.

EIN data element

EIN test functionality was added to the Sybase HIPAA Accelerator maps in a previous release, but implemented such that testing for each element had to be enabled separately. The updated solution provided in Sybase HIPAA Accelerator 6.0 adds parameter 8 to the map, which enables or disables EIN testing at runtime.

EIN testing is disabled as delivered in the product. Enable testing by setting Parameter 8 to 'Y' in ECMAP. See the *ECMAP User's Guide* for details on setting parameters.

Sybase HIPAA Accelerator compliance maps can perform syntax checks on transaction elements containing the Employer Identification Number (EIN). This processing is disabled as delivered from Sybase; however, this section describes how to enable the processing rule.

Table 2-2 illustrates the National Provider Identifier data elements.

Note There are no EIN data elements in the 835 compliance map.

Table 2-2: EIN data elements

Compliance map	Loop/segment ID	HIPAA IG page
270	2100A NM1	46
	2100B NM1	52
	2100C PRV	82
	2100D PRV	123
271	2100A NM1	165
	2100B NM1	180
	2120C NM1	252
	2120C PRV	263
	2120D NM1	329
	2120D PRV	340
276	2100D NM1	75
277	2100D	155
278RQ	2010A NM1	71
	2010B NM1	75
	2010B REF	78
	2010E NM1	154
	2010E REF	155
278RP	2010A NM1	266
	2010B NM1	277
	2010B REF	280
	2010CB NM1	325
	2010DB NM1	376
	2010E NM1	389
	2010E REF	390
	2010F NM1	482
820	1000B N1	61
834	1000A N1	36
	2100D NM1	92
837D	2101AA NM1	76
	2010AA REF	81
	2010AB NM1	86
	2010AB REF	91
	2310A NM1	182
	2310A REF	186
	2310B NM1	189
	2310B REF	193

Compliance map	Loop/segment ID	HIPAA IG page
	2310C NM1	195
	2310D NM1	200
	2330A NM1	230
	2330D REF	255
	2330E REF	259
	2420A NM1	291
	2420A REF	295
	2420C NM1	303
837I	2010AA NM1	76
	2010AA REF	82
	2010AB NM1	92
	2010AB REF	98
	2310A NM1	330
	2310A REF	334
	2310B NM1	337
	2310B REF	339
	2310C NM1	342
	2310C REF	344
	2310E NM1	346
	2310E REF	352
	2330D REF	420
	2330E REF	424
	2330F REF	428
	2330H REF	432
	2420A NM1	465
	2420A REF	468
	2420B NM1	470
	2420B REF	473
	2420C NM1	476
	2420C REF	478
837P	2010AA NM1	83
	2010AA REF	88
	2010AB NM1	97
	2010AB REF	102
	2310A NM1	271
	2310A REF	275
	2310B NM1	278

Compliance map	Loop/segment ID	HIPAA IG page
	2310B REF	282
	2310C NM1	284
	2310C REF	287
	2310D NM1	290
	2310E NM1	298
	2310E REF	300
	2330D REF	362
	2330E REF	366
	2330F REF	370
	2330H REF	378
	2420A NM1	488
	2420A REF	492
	2420B NM1	494
	2420B REF	497
	2420C NM1	498
	2420D NM1	508
	2420D REF	510
	2420E NM1	513
	2420E REF	518
	2420F NM1	524
	2420F REF	528
275 *4050*	2100D NM1	68
277 RQ for additional info	1000C NM1	50
	1000C REF	53

Validating maps against National Employer ID values

As of July 30, 2004 the only valid qualifier for Loop 1000B/N103 should be "65" for the National Employer ID (NEI).

1 Set Parameter 13 to Y to validate against the new NEI value.

2 By adding Parameter 13 to ECMap, users can toggle between default current non-NEI codes and the new NEI value.

Note If you are running ECMap through a gateway, the value of "65" is not accepted in the 820 compliance map. Conversely, other qualifiers (1, 9, 24, 75, EQ, FI and PI) should no longer be valid.

CHAPTER 3

Running and Testing Compliance Maps

About this chapter

Running the map against data involves identifying your inbound EDI data directory and performing additional steps on the Run Inbound Map window before running your map.

This chapter describes how to run a HIPAA compliance map and assumes you have already performed the steps for the compliance map setup described in Chapter 2, “Working with Compliance Maps.”

Contents

Verifying data compliance

Running the map involves identifying the data, map, and logging details and includes the following steps:

1 Run the compliance map. You refer to the directory in which the compliance map was installed.

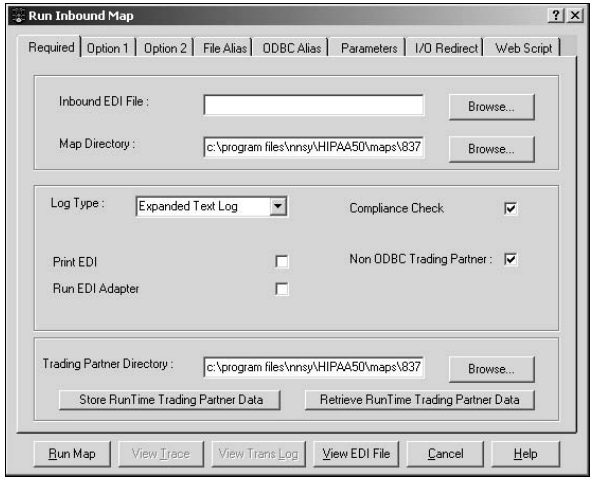
2 Optionally create a functional acknowledgement, using the output of the compliance map (*translog.in*) as the input to the 997 map.

❖ Running compliance maps

This procedure describes the prerequisites and steps to run compliance maps.

1 Open ECMap's and, in the main window, select Build > Run Map from the menu.

The Run Inbound Map window displays with the Required tab active.



2 Identify the incoming map information:

- Inbound EDI File is the full path name of the file containing the EDI data to be translated by the map. You can type the full directory path, including the file name with file extension, or click Browse to locate the file.

- Map Directory is the full path name of the directory containing the generated map (*.map* file). This is the map directory that you defined on the Map Directories tab of the Maps screen, and it is automatically populated by the program. If you choose, you can type a different directory or search for one using the Browse button.
- While the program is processing the EDI data, it places information in a log file. The Log Type specifies how that information is recorded.

  If you set up an ODBC-compliant log database on the Maps DSN tab of the New Map screen when you created the map, the File Type must be ODBC Log.

  If you did not set up an ODBC log database, you have three choices: Text Log, No Log, or Expanded Text Log.

  - If you choose Text Log, the program writes entries to a short log, containing fewer fields than the expanded text log, when the map runs. This selections precludes the ability to run acknowledgements.
  - If you choose No Log, the program does not write entries to the log when the map runs. This selections precludes the ability to run acknowledgements.
  - If you choose Expanded Text Log, the program writes entries to a sequential log file that contains all the same fields as the ODBC log.

  If you plan to build and send a Functional Acknowledgement (997) for the transaction being processed, you must choose either ODBC Log or Expanded Text Log. See the *ECRTP User's Guide* for formats of these log files.
- Select the Compliance Check box if you want to perform a compliance check comparing the EDI data being sent or received with the applicable EDI standard. To use this option, you must generate the map as a compliance map, and you must use CMP as the purpose on the General tab of the Trade Agreement screen.
- Deselect the Print EDI and Run EDI Adapter boxes. See The "Running Map" chapter in the *ECMap User's Guide* for information about these options.
- Select the Non ODBC Trading Partner box if you are *not* using a database for trading partner information. Do not select this check box if you are using an ODBC database.

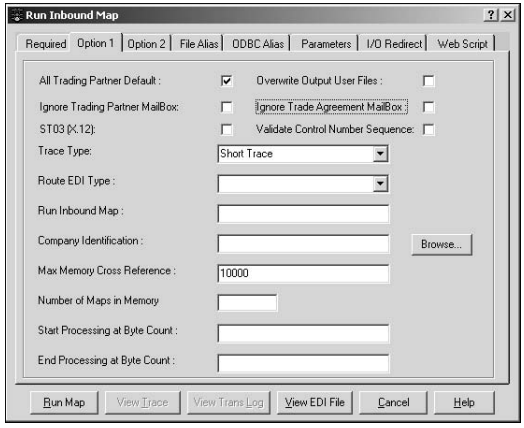
- You can type the directory path in the Trading Partner Directory text box or search by clicking Browse.

Note You must type or browse to the Trading Partner Directory if you checked Non-ODBC Trading Partner. This directory contains your dBase III trading partner (*customer.dbf*) and trade agreement (*tradstat.dbf*) files.

- The Store RunTime Trading Partner Data and Retrieve RunTime Trading Partner Data buttons are enabled if you checked the Non ODBC Trading Partner box.

  Click the Store RunTime Trading Partner Data button the *first time* you set up a compliance map. Otherwise, use these buttons for non-ODBC databases if you are concerned about a disparity between the actual control counts and the control counts that display. See the *ECMap User's Guide* for more information on the Store RunTime Trading Partner Data and Retrieve RunTime Trading Partner Data features.

3 Click the Option 1 tab of the Run Inbound Map window to make it active and supply the following information, where appropriate:



a Select the All Trading Partner Default box.

When All Trading Partner Default is selected, the program defaults to the ALL TradePartner if it does not find a trade agreement for the trading partner when the map runs. This option is useful when:

- Data is first processed through a specific map, such as a compliance map, then processed through an actual map
- Data is received from trading partners that have not been set up or linked with this map

This option allows the data to be processed when no valid trade agreement is in the trading partner database for this data set.

b Leave the Overwrite Output User Files box blank. Compliance maps do not produce user files.

c The Ignore Trading Partner Mailbox, Ignore Trade Agreement Mailbox and Validate Control Number Sequence boxes are significant only for routing EDI. Selecting any of the three affects the location of the EDI output of the map.

- For testing purposes, select these check boxes so that transactions containing data that fails compliance are written to the *bad0.edi* file in the maps directory and not to the mailboxes.
- For production purposes, clear these check boxes so that the pass/fail data is placed in the GOOD/BAD mailboxes.

d Select Short Trace as the Trace Type.

Short Trace produces a listing of only the errors that ECMap encountered during mapping or displays the message:

```
Map run complete. No errors detected.
```

To see more detail, run the map with Long Trace as the Trace Type.

e Route EDI Type is not an available option for compliance maps. EDI Out is always the default choice for compliance maps.

f Ignore Run Inbound Map.

g Type or browse to a value in the Populate the Company Identification text box to associate a specific company profile with this map.

Note If you click Browse, the Select Company ID screen displays a list of the company profiles available. Double-click a profile, and the program enters the profile number associated with the profile in this text box.

---

h The Max Memory Cross Reference text box contains the maximum allowable number of entries in a cross-reference table for memory lookups, with a default of 10,000 entries.

If the entries in any single table exceed the number entered in this text box, then that table is not stored in memory and the lookups for that table go to disk.

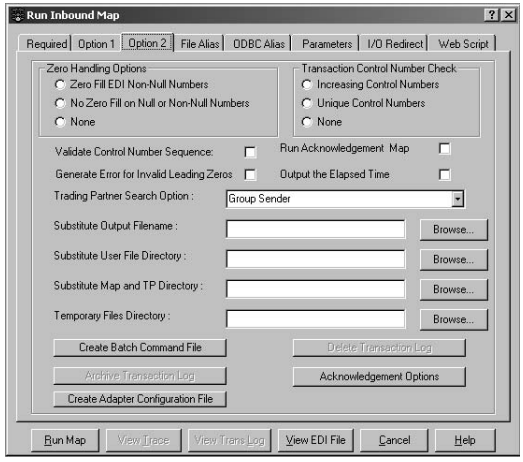
Note This option is ignored when the RTP is run on a UNIX machine, where all tables are stored in memory.

---

i Start Processing at Byte Count is used to designate the specific character (byte) at which processing of the incoming EDI file begins. When only specific portions of large data files need to be processed, this option saves the time of reading through the preceding data.

j End Processing at Byte Count is used to designate the specific character (byte) at which processing of the incoming EDI file ends. When only specific portions of large data files need to be processed, this option saves the time of reading through the subsequent data.

4 Click the Option 2 tab of the Run Inbound Map window to make it active, and identify the following information:



a Compliance maps assume that Zero Fill EDI Non-Null Numbers is selected. When selected, the program fills with zeroes incoming numeric elements that are not blank. This is the `-z` switch on the command line.

b Select the Create Bad Transaction Log box.

Warning! You must select this check box to create the file that contains failed translation data.

c To save the elapsed time of the run into a trace file, select Output the Elapsed Time box. This is an option only when you use Short Trace.

d To optionally create 997 information, select the Run Acknowledgement Map check box. The Build Acknowledgement window displays.

e The Trading Partner Search Option specifies which sender and receiver fields in the incoming EDI envelopes the trading partner lookup uses. See the *ECMap User's Guide* for more detailed information on this option.

f Ignore the Substitute Output Filename. It is not applicable for compliance maps since they do not produce an output file.

g Ignore the Substitute User File Directory. It is not applicable for compliance maps since they do not produce an output file.

h Ignore the Substitute Map and TP Directory. It is not specific to compliance maps.

i Ignore the Temporary Files Directory field.

j Click Create Batch Command File to create a batch command file that automatically runs the map once you have set all the switches and options.

k Click Delete Transaction Log to create a new log of compliance data that is related only to the map you are currently running.

Note This option is valid for the expanded text log. If you are testing with the ODBClog, you must manually delete rows in the TRLOG table during testing.

Delete Transaction Log permanently removes the contents of the transaction log file. Since new entries to the transaction log are appended to existing entries, rather than overwriting them, it is important to control the size of this log by periodically purging the contents. If you want to save the contents of the log, you should archive it prior to deleting it. Once you have deleted the log, you cannot recover it. You receive no message saying that the log has been deleted.

- Click Acknowledgement Options only to modify existing acknowledgement options or to view the output generated from a run with acknowledgements.

5 You are now ready to run data through the compliance map. Click Run Map.

Support for HCCO CCAP testing

Sybase HIPAA Accelerator implementation adheres to a careful interpretation of the gray box rules, called Industry Notes in the HIPAA Implementation Guides. Because these rules are subject to different interpretations, Sybase is involved with HIPAA Conformance Certification Organization Common Conformance Assessment Program (HCCO CCAP), whose interoperability testing assists vendors in interpreting the Implementation Guides in the same manner, regardless of the tools they use to process their claims.

Sybase HIPAA Accelerator's HIPAA compliance maps support the following changes to the December 2003 HCCO CCAP test suites:

- The removal of errors for trailing spaces, warnings are recommended but not a violation
- The removal of errors for leading zeroes, warnings are recommended but not a violation
- The presence of empty segments; for example, N4 present but without data is compliant
- The presence of extra data; for example, NM104 present but not required when a "1" is compliant

CHAPTER 4

Troubleshooting Map Errors

About this chapter

Errors that result from noncompliant data in the message are captured in the ECMap transaction log. This information can be used to quickly identify the data that is in error and its location within the transaction.

The following errors are common errors that may be trapped by the HIPAA compliance maps. Refer to the *ECMap Reference Guide* for a complete list and explanation of messages.

Contents

Handling noncompliance errors

After running the map, use the error trapping and display features in ECMap to view the results of the compliance check.

To resolve errors, use the segment and element tags to look up the required information in the Detail portion of the HIPAA Implementation Guide associated with your map.

Viewing the transaction log for an inbound map

The View Trans Log button lets you retrieve information that ECMap places in the log file. The amount of information in the log depends on the Log Type option (Text Log, No Log, or Expanded Text Log) that you selected on the Required tab of the Run Inbound Map window.

The transaction log tells you whether the map ran successfully or failed, but it also performs other functions. For example, the results of Write Log rule commands that the map used display. If you are using a 997 functional acknowledgement, the 997 uses *translog.in* as input. When you select View Trans Log, the translog.in – Notepad window displays for non-ODBC logs and the View Transaction Log with Run ID: <run ID #> window displays for ODBC logs.

The following information also displays:

- A list of the errors and warnings that occurred during map execution
- The results of user-generated entries created with Write Log rule commands
- System-generated messages for each ST and SE segment

Viewing the EDI file for an inbound map

The View EDI File button displays the EDI Viewer window where you can print the EDI file, find character strings in the file, replace character strings, view the file in a wrapped or unwrapped format, and save the file. You can edit the EDI file if required, such as when errors occurred that required correction. You can also open another EDI file and perform the same operations on it.

From the File menu on the EDI Viewer window, you can open another EDI file (or any file), save (or Save As) the open file, or print the open file.

- When you choose Open from the File menu on the EDI Viewer window, the Browse – EDI File window displays.

  From the Edit menu, either Find a character string or find a string and Replace it with another character string.

- If you choose Find, the Find dialog box displays. Type the character string you want to find in the Find What text box and click Enter. The character string for which you are searching displays as highlighted. To find another occurrence of the character string, click Find Next or Cancel to exit.

- If you choose Replace, the Find dialog box displays with a new Replace With text box. Type the character string you want to replace in the Find What text box and the character string to be substituted in the Replace With text box.

  Click the Replace key. The character string is replaced, displayed, and highlighted. To replace another occurrence of the character string, click Find Next and then Replace again. To exit the dialog box, click Cancel.

  From the Options menu, view EDI in a blocked or an unblocked format.

- If you choose to view the EDI file in a blocked format, the EDI Block Size dialog box displays. In the text box, type a block size between 40 and 300 and click OK. The EDI file in the EDI Viewer window now displays in blocks of the length you just specified.

Viewing the transaction log for an outbound map

The View Trans Log button lets you review the information in the log file. The amount of information in the log depends on the Log Type option (Text Log, No Log, or Expanded Text Log) that you selected on the Required tab of the Run Outbound Map window.

The transaction log tells you whether the map ran successfully or failed, but it also performs other functions. For example, the results of Write Log rule commands which map displays. When you select View Trans Log, the translog.out – Notepad window displays for non-ODBC logs and the View Transaction Log with Run ID: <run ID #> window displays for ODBC logs.

The following information also displays:

- A list of the errors and warnings that occurred during map execution
- The results of user-generated entries created with Write Log rule commands

- System-generated messages for each ST and SE segment

Viewing the EDI file for an outbound map

From the Run Outbound Map window, you can select View EDI File to display the EDI Viewer window. On this window, you can print the EDI file, find character strings in the file, replace character strings, view the file in a wrapped or unwrapped format, and save the file. You can edit the EDI file if required, such as when errors occurred that required correction. You can also open another EDI file and perform the same operations on it.

From the File menu on the EDI Viewer window, you can open another EDI file (or any file), save (or Save As) the open file, or print the open file.

- When you choose Open from the File menu on the EDI Viewer window, the Browse – EDI File window displays.

  From the Edit menu, you can either find a character string or find a string and replace it with another character string.

- If you choose Find, the Find dialog box displays.

  a Type the character string to find in the Find What text box and click Enter. The character string for which you are searching is highlighted.

  b To find another occurrence of the character string, click Find Next or Cancel to exit.

- If you choose Replace, the Find dialog box displays with a new Replace With text box.

  a Type the character string to replace in the Find What text box and the character string to be substituted in the Replace With text box.

  b Click Replace. The character string is replaced, displayed, and highlighted.

  c To replace another occurrence of the character string, click Find Next and then Replace again.

  d Click Cancel to exit.

  From the Options menu, you can choose to View EDI in a Blocked or an Unblocked format.

- If you choose to view the EDI file in a blocked format, the EDI Block Size dialog box displays. In the text box, type a block size between 40 and 300 and click OK. The EDI file in the EDI Viewer window now displays in blocks the length that you just specified.

  The EDI data displays in an unwrapped format. Each segment begins on a separate line and has an incremental line number. In addition, position markers that appear above every 10th character help you to easily identify the character positions within the segments.

  You can wrap the unwrapped EDI data by clicking Wrap EDI. The EDI data appears as one long wrapped record on the EDI Viewer window.

- If you select Options on the EDI Viewer window, the Options window displays. On the Options window, you can set the starting character (Start Byte), the ending character (End Byte), and length (Wrap Size) of the EDI records you are viewing.

For details on viewing and correcting errors, see the *ECMap User's Guide* and the *ECMap Reference Guide*.

Map error types

The following are the error types that compliance maps capture. Since you can add error checking for your own business rules, this section does not represent a complete list.

Common compliance scenarios and responses

This section describes common compliance errors and their responses. Although the descriptions represent typical error scenarios, the list is not all inclusive, and you may encounter different errors for which you should contact your Sybase technical representative.

Table 4-1: Map error scenario 1

Description	Map response
When NM101 NE IL is in loop 2100A, the map reports: `Segment not found` The map should report on the specific error; for example, NM101 in loop must equal IL.	The logic that the map follows will not get to the mapping for the NM1 in which loop 2100A is defined because the qualifier is not an IL (a valid value). Therefore, the map produces a generic error message.

Table 4-2: Map error scenario 2

Description	Map response
In the 837I map, an Invalid Error on REF Loop 2010AA processes the second REF at the incorrect level.	The 837I Implementation Guide contains errors, where the same code for both REF segment definitions and the REF segments in this instance are defined one after the other. Therefore, there is no logical way to determine which REF is correct.

Table 4-3: Map error scenario 3

Description	Map response
In the 834 map, the map reports no errors on N1 qualifiers in Loop 1000. Instead, the user sees the following message: `Not found in master segment table` Flow points have element qualifiers. Therefore, if the qualifier is wrong, it does not move to the N1 level; thus, the map reports no specific error.	The logic that the map follows will not get to the mapping for the NM1 in which loop 2100A is defined because the qualifier is not an IL (a valid value). Therefore, the map produces a generic error message.

997 errors

The following are the error types linked to specific 997 output that compliance maps capture. Since you can add error checking for your own business rules, this is not an exhaustive list.

For more information, see the chapter, “Working with Rules,” in the *ECMap User’s Guide*.

2029 error

This section lists the description, cause, and action to take regarding the 2029 compliance map error.

- Description: Segment exceeding maximum occurrence.
- Cause: Violation of the gray box rules as described in the HIPAA Implementation Guide.
- Action: Change incoming data or instruct the submitter of the data to provide a value in the field.

Map	Example of text error messages for error code 2029
270	Not applicable
271	Not applicable

276	`Received more than one REF segment (REF01=1K) in the loop`
	`Received more than one REF segment (REF01=BLT) in the loop`
	`Received more than one REF segment in loop 2200D where REF01`
	`The maximum number of REF segments in loop 2200D has been exceeded`

277	`The maximum number of REF segments in loop 2200D has been exceeded`
278RQ	Not applicable
278RP	Not applicable
820	Not applicable
834	Not applicable

835	`2100-REF, Exceeds 10 Occur`
	`2100-REF, Exceeds 5 Occurrence`
	`2100-NM101=PR, Exceeds 2 Occur`
	`2110-REF Exceeds 10 Occur`
	`2110-REF Exceeds 7 Occur`

837D	`2320 SBR Loop count exceeds 10`
	`2300 CLM Loop count exceeds 100`
	`2400 LX Loop count exceeds 50`
	`2430 SVD Loop count exceeds 25`

Map	Example of text error messages for error code 2029
837I	2010AA-1st REF OCCURS > 8 Time 2010AA-2nd REF OCCURS > 8 Time 2010CA-REF Occurs GT 5 Times 2300-More than 1 AMT01=C5 2300-More than 1 AMT01=F3 2300-More than 1 AMT01=F5 2300-More than 1 AMT01=MA 2300-More than 1 DTP01=096 2300-More than 1 DTP01=434 2300-More than 1 DTP01=435 2300-More than 1 HI0101=BK 2300-More than 1 HI0101=DR 2300-More than 1 HL0101=BPorBR 2300-More than 1 NTE Segment 2300-More than 1 REF01=4N 2300-More than 1 REF01=9A 2300-More than 1 REF01=9C 2300-More than 1 REF01=D9 2300-More than 1 REF01=DD 2300-More than 1 REF01=EA 2300-More than 1 REF01=F8 2300-More than 1 REF01=G4 2300-More than 1 REF01=LX 2300-More than 1 REF01=P4 2300-More than 10 NTE Segments 2300-More than 2 CRC01=77 Seg 2300-More than 2 HI0101=BE 2300-More than 2 HI0101=BG 2300-More than 2 HI0101=BH 2300-More than 2 HI0101=BI 2300-More than 2 HI0101=TC 2300-More than 2 HI0101-BOorBQ 2300-More than 2 REF01=9ForG1 2300-More than 3 CRC01=75 Seg 2300-More than 3 CRC01=76 Seg 2310-More than 1 NM101=71 2310-More than 1 NM101=72 2310-More than 1 NM101=73 2310-More than 1 NM101=FA 2330-AMT Occurs More Than Once 2330A-NM101=IL Occurs > 1 2330B: REF Occurs > 1

Map	Example of text error messages for error code 2029
837I (continued)	2330B:REF Occurs > 2 2330B-NM101=PR Occurs > 1 2330C NM101=QC Occurs > 1 2330D: NM1=71 Occurs > 1 2330E:NM101=72 Occurs > 1 2330F: NM101=73 Occurs > 1 2330H:NM101=FA Occurs > 1 2400 -DTP01=472 Occurs > 1 2400-AMT01=GT Occurs > 1 2400-AMT01=N8 Occurs > 1 2400-DTP01=866 Occurs > 1 2420-NM101=71 Occurs > 1 2420-NM101=72 Occurs > 1 2420-NM101=73 Occurs > 1
837P	2300 DTP Seg Exceeds Max Occur 2300 REF Seg Exceeds Max Occur 2310A NM1 Seg Exceeds MaxOccur 2310ANM1 DN SegExceedsMaxOccur 2310ANM1 P3 SegExceedsMaxOccur 2310B NM1 Seg Exceeds MaxOccur 2310C NM1 Seg Exceeds MaxOccur 2310D NM1 Seg Exceeds MaxOccur 2310E NM1 Seg Exceeds MaxOccur 2320 AMT Seg Exceeds Max Occur 2330 NM1 Seg Exceeds Max Occur 2330B REF Seg Exceeds MaxOccur 2330D NM1 DN SegExceedsMaxOccur 2400 AMT Seg Exceeds Max Occur 2400 CRC Seg Exceeds Max Occur 2400 DTP Seg Exceeds Max Occur 2400 REF Seg Exceeds Max Occur

2045 error

This section lists the description, cause, and action to take regarding the 2045 compliance map error.

- Description: Invalid date and time field format.
- Cause: Date in the data file does not match the format specified in the compliance map.
- Action: Change incoming data to meet specified format.

Map	Example of text error messages for error code 2045
270	DTP03 Length NE 17, RD8 Length DTP03 Length NE 17, Invalid RD8 DTP03 Length NE 8, Invalid D8 DTP03 NE 17, Invalid RD8 DTP03 NE 8, Invalid D8 Invalid D8 - Date Length Invalid DTP03 Length, DTP02=D8 Invalid RD8 - Date length to_date < from_date ! allowed
271	DTP03 length ne 17 DTP03 length ne 8 To_date < from_date ! Allowed
276	Date form does not = YYYYMMDD Invalid date range RD8 Length checked failed
277	Date form does not = YYYYMMDD Incorrect date range Invalid date range
278RQ	2000F CR604 Date format wrong 2000F CR616 Date format wrong 2000F DTP/435 format incorrect 2000F DTP/472 format incorrect 2000F HI0104 Date format wrong 2000F HI0204 Date format wrong 2000F HI0304 Date format wrong 2000F HI0404 Date format wrong 2000F HI0504 Date format wrong 2000F HI0604 Date format wrong 2000F HI0704 Date format wrong 2000F HI0804 Date format wrong 2000F HI0904 Date format wrong 2000F HI1004 Date format wrong 2000F HI1104 Date format wrong 2000F HI1204 Date format wrong
278RP	To_date < from_date Incorrect length for D8 Incorrect length for RD8 Invalid D8 format
820	Date Format must be YYYYMMDD Invalid length for date range To_date < from_date ! allowed
834	Not applicable

Map	Example of text error messages for error code 2045
835	Not applicable
837D	2300-Invalid TM where DTP02=DT DTP 434 Stmt Dates required
837I	2300:DTP01=472 Invalid Date 2300-Invalid TM where DTP02=DT DTP 434 Stmt Dates required
837P	2300 - Invalid Time Format 2400 DTP03 is wrong length To Date cannot be less than From Date Wrong length Wrong tm: HH Wrong tm: MM

2169 error

This section lists the description, cause, and action to take regarding the 2169 compliance map error.

- Description: Empty value mapped to EDI mandatory field.
- Cause: Information on a required element within a segment is missing in the inbound data.
- Action: Add element information in the specified location of the segment.

Map	Example of text error messages for error code 2169
270	2100A_NM104 required if NM1=1 2100B_NM104 required if NM1=1 2100B_REF01=0B, REF03 required NM104 is invalid when 2100B level NM102 equals 2 NM105 is invalid when 2100B level NM102 equals 2 NM107 is invalid when 2100B level NM102 equals 2
271	PER02 absence mandates PER04 REF01 value mandates REF03
276	2100B_NM104 must be present 2100C_NM104 is required 2100D_NM104 is required
277	Not applicable
278RQ	2010A - NM104 is blank 2010B - NM104 is blank

Map	Example of text error messages for error code 2169
278RP	2000F HCR01=A1/HCR02 null 2000F HCR01=A3/HCR03 null 2000F HCR01=A4/HCR03 null 2000F HCR01=A6/HCR02 null 2010A-NM104 is blank 2010B-NM104 is blank
820	04=ACH: 05-09,12-19 must exist
834	INS01=Y, 08 must contain data NM102=1, 03/04 must have data
835	Not applicable
837D	DMG in Loop 2320 is Missing DTP=330 Seg In 2300 is Missing DTP=435or 096 Seg 2300 Missing DTP=439 Accident Seg Missing DTP=441 Seg In 2400 is Missing If CLM11_1,2or3=AA, 04 is Req IF PWK02=EM,EL,BM,FX;05 is Req IF PWK02=EM,EL,BM,FX;06 is Req If SBR09=MB, CLM07 is required NM1 Segment in 2310C Missing NM104 is Required when NM102=1 NM108 is Required when NM102=1 NM109 is Required when NM102=1 REF Segment in 2310A Missing REF=F8 Segment in 2300 Missing SBR02=18, DMG in 2010BA is Req SBR02=18, N3 in 2010BA is Req SBR02=18, N4 in 2010BA is Req
837I	Not applicable
837P	Not applicable

2190 error

This section lists the description, cause, and action to take regarding the 2190 compliance map error.

- Description: EDI Envelope data in error.
- Cause: Information on a required element within an envelope segment is missing in the inbound data.
- Action: Add element information in the specified location of the segment.

Map	Example of text error messages for error code 2190
All Maps	`Invalid GS01 element` `Invalid GS08 element`

2191 error

This section lists the description, cause, and action to take regarding the 2191 compliance map error.

- Description: EDI envelope data in error.
- Cause: Information on a required element within an envelope segment is missing in the inbound data.
- Action: Add element information in the specified location of the segment.

Map	Example of text error messages for error code 2191
All Maps	`Invalid ST01 element`

2350 error

This section lists the description, cause, and action to take regarding the 2350 compliance map error.

- Description: Invalid data in element.
- Cause: Violation of gray box rules as described in the HIPAA Implementation Guide.
- Action: Change incoming data or instruct the submitter of the data to provide a value in the field.

Map	Example of text error messages for error code 2350
270	Not applicable

Map	Example of text error messages for error code 2350
271	2000A - Invalid HL01 value 2000B - Invalid HL01 value 2000B - Invalid HL02 value 2000C - Invalid HL01 value 2000C - Invalid HL02 value 2000D - Invalid HL01 value 2000D - Invalid HL02 value AAA03 must be 42 for AAA04 = R AAA03 must be 42 for AAA04 = Y EB01 val disallows REF01 val Invalid 2110C LE01 value, must be 2120 Invalid 2110D LE01 value, must be 2120 NM102 NE 1, NM104 disallowed NM102 NE 1, NM105 disallowed NM102 NE 1, NM107 disallowed PER02 empty, PER04 required PER03 mandates numeric PER04 PER05 mandates numeric PER06 PER07 mandates numeric PER08 TRN03 must start w/ 1, 3, or 9
276	2100B_NM102=2, check NM104/05 2210D_SVC04 not used SVC01=NU 2210E_SVC04 not used SVC01=NU HL has invalid value Phone # should be numeric
277	2100B_NM102=2, check NM104/05 2100C_NM102=2, check NM104/04 2100C_NM102=2, check NM104/05 2220C_SVC04 not used SVC01=NU 2220E_SVC04 not used SVC0=NU Hl has invalid value Phone# length should be 10 Phone# should be numeric

Map	Example of text error messages for error code 2350
278RQ	2000A HL01 count incorrect 2000B HL01 count incorrect 2000B HL02 count incorrect 2000C HL01 count incorrect 2000C HL02 count incorrect 2000C PWK05 & PWK06 must both be present or blank 2000C PWK05 is required when PWK02 is not 'AA' or 'VO' 2000C TRN03 is incorrect 2000D HL01 count incorrect 2000D HL02 count incorrect 2000D PWK05 & PWK06 must both be present or blank 2000D PWK05 is required when PWK02 is not 'AA' or 'VO' 2000D TRN03 is incorrect 2000E HL01 count incorrect 2000E HL02 count incorrect 2000F CR103 NE X, CR109 valued 2000F CR103=X, CR109 NULL 2000F CR106/CR107 not present 2000F CR106/CR108 not present 2000F CR201 valued/CR202 NULL 2000F CR205=MO/CR207 empty 2000F CR503/CR518 empty 2000F CR510/CR511 empty 2000F CR516 empty 2000F HL01 count incorrect 2000F HL02 count incorrect 2000F PWK05 & PWK06 must both be present or blank 2000F PWK05 is required when PWK02 is not 'AA' or 'VO' 2000F TRN03 is incorrect 2000F UM01=HS/CR208 empty 2000F UM01=HS/CR209 empty 2000F UM0503 not valued 2000F UM0503, UM0501/02 NULL 2000F UM06 empty when UM02=1 2010B PER02 NULL/PER03 NULL 2010B PER02 NULL/PER04 NULL 2010B NM102=2/NM105 NE NULL

Map	Example of text error messages for error code 2350
278RQ (continued)	2010B NM102=2/NM107 NE NULL 2010B REF01=EI when NM108=24 2010B REF01=SY when NM108=34 2010C NM108=MI/REF01=1W 2010E PER02 NULL/ PER04 NULL 2010E PER02 NULL/PER03 NULL 2010E NM102=2/NM105 NE NULL 2010E NM102=2/NM107 NE NULL 2010E NM104 NULL/NM103 Present 2010E REF01=EI when NM108=24 2010E REF01=SY when NM108=34
278RP	2000A HL01 count incorrect 2000B HL01 count incorrect 2000B HL02 count incorrect 2000C AAA01=N/ AAA03 null 2000C AAA03 present AAA04 null 2000C HL01 count incorrect 2000C HL02 count incorrect 2000C TRN03 is incorrect 2000D AAA01=N/ AAA03 null 2000D AAA01=N/ AAA04 null 2000D HL01 count incorrect 2000D HL02 count incorrect 2000D PWK05 & 06 must be present or blank 2000D PWK05 is required when PWK02 is not 'VO' 2000D TRN03 is incorrect 2000E HL01 count incorrect 2000E HL02 count incorrect 2000F AAA01=N/ AAA03 null 2000F AAA03 present AAA04 null 2000F CR205=MO/CR207 empty 2000F CR503/CR518 empty 2000F CR516 empty 2000F HL01 count incorrect 2000F HL02 count incorrect 2000F PWK05 & 06 must both be present or blank 2000F PWK05 is required when PWK02 is not 'VO' 2000F TRN03 is incorrect 2000F UM06 empty when UM02=12010A - PER03 is blank 2010A PER04 is blank 2010A AAA01=N/ AAA03 null

Map	Example of text error messages for error code 2350
278RP (continued)	2010A AAA03 present AAA04 null 2010A NM102=2/NM105 NE NULL 2010A NM102=2/NM107 NE NULL 2010B AAA01=N/ AAA03 null 2010B AAA03 present AAA04 null 2010B REF01=EI when NM108=24 2010B REF01=SY when NM108=34 2010C AAA01=N/ AAA03 null 2010C AAA03 present AAA04 null 2010C NM108=MI/REF01=1W 2010CB N4 05 & 06 must both be present or blank 2010D AAA01=N/ AAA03 null 2010D AAA03 present AAA04 null 2010DB N4 05 & 06 must both be present or blank 2010E PER03 is blank 2010E PER04 is blank 2010E AAA01=N/ AAA03 null 2010E AAA03 present AAA04 null 2010E NM104 NULL/NM103 Present 2010E REF01=EI when NM108=24 2010E REF01=SY when NM108=34 phone# should be numeric
820	BPR02 cannot be Negative BPR10 not precede by Value '1' Data not required Invalid phone number MaxLength in BPR02 exceeded MaxLength in REF02 exceeded Must be preceded by Value '1' TRN03 not equal BPR10 TRN04 not equal BPR11

Map	Example of text error messages for error code 2350
834	2000 REF Member Identification Number out of sequence 2000 REF Member Policy Number out of sequence 2000 REF Prior Coverage Months out of sequence DMG04 contains data, INS01!=Y DMG05 contains data, INS01!=Y DMG06 contains data, INS01!=Y DSB08 Must equal 585 DTP01 = 349, HD01 = 024 HD05 not used if INS01 not=Y If BGN06 exist, BGN01 != 00 INS01 != Y, REF01 = 17 INS01 = Y, INS02 = 18 INS03 != 030 INS05 != C, INS07 = empty Mandatory 2000 REF Subscriber Number not first REF, or not N406 contains data, INS01 != Y NM103,4,5 in 2100A/B must EQ Phone# should be all digits REF01 contains data, INS01!=Y Req data INS06 not match 08
835	2103.NM105 may not be used 2103.NM107 may not be used 2103_NM104 may not be used 2104.NM104 may not be used 2104.NM105 may not be used 3200.CLP03 - CASall != CLP04 BPR04 != ACH, BPR05 disallowed H.3510 MIA or MOA, not both H.TRL sumCLP04 - sumPLB NE BPR HDR.BPR02 less than zero HDR.BPR02 more than 11 chars HDR.BPR04 must be NON HDR.BPR10 not preceeded by "1" HDR.TRN03 != BPR10 HDR.TRN03 not preceeded by "1" HDR.TRN04 != BPR11 MV_BPR_202MV_CLP04s - PLBamounts MV_CLP04sum MV_PLBsumamount phone# should be all numeric SVC not EQ CAS

Map	Example of text error messages for error code 2350
837D	DTP in 2330B Segment is required when DTP in 2430 is missing HL01 not in right sequence HL02 in 2000B, Wrong Parent ID HL02 in 2000C, Wrong Parent ID If NM108=MI in 2010BA, REF!=1W If NM108=XX, REF01=EI,SY or TJ If NM108=XX, REF01=EI,SY or TJ Invalid Value in LX01 Invalid value in REF02 Header Length of CLM1 can't exceed 20 Loop ID 2310D: The value in element NM102 was equal to 1 but element NM104 was empty Loop ID 2420C: The value in element NM102 was equal to 1 but element NM104 was empty NM104 Should Be Empty NM105 Should Be Empty NM107 Should Be Empty NM109 2420B Must Match 2330B NM109 2420B Must Match SVD01 REF in 2330A is used only when SBR in 2320 is used REF02 Length can't exceed 20 SBR09=MB, REF01=SY is not a valid segment

Map	Example of text error messages for error code 2350
837I	1000A_NM102 disallows NM105 1000A_NM102 val mandates NM104 1000A_PER04 is non-numeric 1000A_PER06 is non-numeric 1000A_PER08 is non-numeric 2000A Invalid HL01 value 2000B Invalid HL01 value 2000B Invalid HL02 value 2000B-SBR09 Empty 2000C Invalid HL01 value 2000C Invalid HL02 value 2010AA_PER04 is non-numeric 2010AA_PER06 is non-numeric 2010AA_PER08 is non-numeric 2010BA_NM102 disallows NM105 2010BA_NM104 required 2010BA_NM108 required 2010BA_NM109 is required 2010BA-NM102 Disallows NM107 2010BB_NM102 disallows NM105 2010BB_NM104 required 2010BB-NM102 disallows NM107 2010BD: NM102 disallows NM107 2010BD_NM102 disallows NM105 2010BD_NM104 is required 2010CA - pt. info missing2300 - Invalid Date Format 2300: Invalid RD8 Format2300: Invalid RD8 Format 2300 Missing Admitting Diag 2300 Warning CLM01>20 2300 CR616 Invalid Date 2300 CR616 Invalid Date Range 2300_CR604 Date Range Invalid 2300_CR604 Invalid Date Range 2300_PWK02 val mandates PWK05 2300_PWK02 val mandates PWK06 2300-Invalid Claim-No LX 2300-Invalid HHMM Format 2300-Invalid Time - Hour 2300-Invalid Time-Minute 2310A NM107 Contains Data

Map	Example of text error messages for error code 2350
837I (continued)	2310A_NM102 disallows NM105 2310A_NM104 required 2310C NM107 Must Be Blank 2310C_NM102 disallows NM105 2310C_NM104 required 2320 SBR09 Empty 2330A NM107 Must Be Empty 2330A_NM102 disallows NM105 2330A_NM104 required 2400 Invalid value LX01 2400 SV206 Empty 2400_Invalid Date in DTP03 2400_PWK02 val mandates PWK05 2400_PWK02 val mandates PWK06 2420A NM107 Not Empty 2420A_NM102 disallows NM105 2420A_NM104 required 2420C Invalid entry in NM105 if NM102=Non Person 2420C Invalid entry in NM107 if NM102=Non Person 2420C Missing Mandatory NM104 when NM101=1 2420C NM107 Not Empty

Map	Example of text error messages for error code 2350
837P	2000A Invalid Value in HL01 2000B HL04 should contain 1 2000B Invalid Value in HL01 2000B Invalid Value in HL0 2200B Medicare-SBR05 empty 2000C Invalid Value in HL01 2000C Invalid Value in HL0 2300 CLM10 Should contain data 2300 CLM1104 must contain data 2300 CR109 Required,CR103=X 2300 HI0102 contains a period 2300 HI0202 contains a period 2300 HI0302 contains a period 2300 HI0402 contains a period 2300 HI0502 contains a period 2300 HI0602 contains a period 2300 HI0702 contains a period 2300 HI0802 contains a period 2300 PWK05 Must Contain Data 2300 PWK06 Must Contain Data 2300 REF02 Len GT 20,REF01=D9 2320 OI04 Empty, Required CR109 Required, since CR103=X Loop 2300 EPSDT Referral - CRC LX01 Contains an Invalid Value Missing Mandatory DMG Segment - Loop 2320 Missing Mandatory DMG Segment - SBR02=18 Missing Mandatory N3 Segment - SBR02=18 Missing Mandatory N4 Segment - SBR02=18 More than 5000 Claims in Transactions N2 Segment should not be present, Length of NM103 NE 35 NM103 in Loop 2310D Cannot be Empty NM104 Should Not Be Empty NM105 Should Be Empty NM107 Should Be Empty NM108 Should Not Be Empty NM109 Should Not Be Empty PER04 contains non numeric data PER06 contains non numeric data PER08 contains non numeric data PRV in loop 2000A or 2310B should be present

Map	Example of text error messages for error code 2350
837P (continued)	REF01=1W cannot be present when NM108=M1 REF01=1W cannot be present when NM108=M1 REF01=SY is invalid in loop 2310n SBR02 Must Equal 18 - HL04 = 0 SBR09=MB, REF01=SY is not a valid segment SV10701 must contain data since HI segment is present The data in CLM01 is greater than 20, some systems may truncate The value in loop 2420G NM109 was not equal to the value in loop 2330B NM109 The value in loop 2430 SVD01 was not equal to the value in loop 2330B NM109 When DTP01=439 present, CLM11 must contain data

2360 error

This section lists the description, cause, and action to take regarding the 2360 compliance map error.

- Description: Invalid segment.
- Cause: Violation of gray box rules as described in the HIPAA Implementation Guide.
- Action: Change incoming data or instruct the submitter of the data to provide a value in the field.

Map	Example of text error messages for error code 2360
270	Not applicable
271	Not applicable
276	Missing mandatory NM1 element No DTP segment was found in either the 2200D or 2210D Subscriber No DTP segment was found in either the 2200E or 2210E loops The 2200E REF segment, REF01=1K is invalid The subscriber is not the patient, but a DMG segment was present The subscriber is the patient, but no DMG segment was present

Map	Example of text error messages for error code 2360
277	2100B_NM102=1, NM104 is used 2100C NM104 required if NM1=1 2100D_NM104 required if NM1=1 A DMG segment was found in Loop 2000D when the subscriber was not the patient Missing NM1 for HL 03 = 23 Missing TRN for HL 03 = 23 No DMG segment found in Loop 2000D when subscriber is the patient Received more than one REF segment (REF01=1K) in the loop Received more than one REF segment (REF01=BLT) in the loop Received more than one REF segment (REF01=EA) in the loop The subscriber is the patient but the TRN segment in loop 22
278RQ	2000C DTP*439 empty/UM0501=AA 2000CorD:DTP Exceeds Max 2000D DTP*439 empty/UM0501=AA 2000F CL1 present/UM01 NE AR 2000F DTP Exceeds Max Occur 2000F DTP Exceeds Occurrence
278RP	> 1 DTP01 = 007 ! allowed > 1 DTP01 = 036 ! allowed > 1 DTP01 = 096 ! allowed > 1 DTP01 = 102 ! allowed > 1 DTP01 = 435 ! allowed > 1 DTP01 = 456 ! allowed > 1 DTP01 = 472 ! allowed 2000CorD:DTP Exceeds Max Occur
820	Not applicable
834	2100E NM1 Loop Occurs > 3 1100C N1 Loop Occurs > 2 2000 REF Mem ID > 5 2000 REF01-OF Occurs > 1 2000 REF-IL Occurs > 1 2100A NM1 Loop Occurs > 1 2100B NM1 Loop Occurs > 1 2100C NM1 Loop Occurs > 1 2100F NM1 Loop Occurs > 1 2100G NM1 Loop Occurs > 1 2100D NM1 Loop Occurs > 3

Map	Example of text error messages for error code 2360
835	Not applicable
837D	2010AA 1st REF Occurs > 5 2010AA 2nd REF Occurs > 8 2010BA 1st REF Exceed Max Occur 2010BA 2nd REF > 1 2010CA 1st REF Occurs > 5 2010CA 2nd REF Occurs > 1 2300 DTP Segment Exceed Occur 2300 REF Exceeds Max Occur 2320 AMT Seg Occur Violation 2330B REF Exceeds Max Occur 2400 DTP Occurs > 1 2400 REF Occurs > 1

Map	Example of text error messages for error code 2360
837I	1000B missing mandatory seg 2000B SBR04 is required if SBR03 is Empty 2010AA REF01=SY Invalid 2010AA_REF01 cannot be SY 2010AA_REF01 must be EI or SY 2010AB REF01=SY Invalid 2010AB_REF01 cannot be SY 2010AB_REF01 must be EI or SY 2010BA_DMG segment required 2010BA_N3 segment required 2010BA_N4 segment required 2010BA_REF01 cannot be SY 2010BA_REF01 may not be 1W 2010BA-REF01=1W Invalid 2010CA_REF01 cannot be SY 2010CA-REF01=1W Invalid 2310A_REF01 cannot be SY 2310A-Medicare REF01=SY Invalid 2310B Medicare REF01=SY Invalid 2310B_REF01 cannot be SY 2310C Medicare,REF01=SY Invalid 2310C_REF01 cannot be SY 2320 Missing Mandatory DMG 2320B Required segment missing 2330A Missing Required N4 2330A REF01=SY InvalidMedicare 2330A_REF01 cannot be SY 2330A_REF01 may not be 1W 2330B Missing Required N4 2330C Medicare-REF01=SY Invalid 2330C_REF01 cannot be SY 2330C_REF01 may not be 1W 2330F REF01=SY Invalid-Medicare 2330F_REF01 cannot be SY 2420A missing mandatory seg 2420A_REF01 cannot be SY 2420B_REF01 cannot be SY 2420C_REF01 cannot be SY Assessment Date DTP is not used when this segment present DTP 434 mandatory seg missing No. Of CLM Seg < 5000 REF01=SY Invalid For Medicare Claim

Map	Example of text error messages for error code 2360
837P	2000A 1st REF Occurs > 8 2000A 2nd REF Occurs > 8 2010AA - Missing Mandatory REF 2010BA 1st REF Occurs > 4 2010BA 2nd REF Occurs > 1 2010CA 1st REF Occurs > 1 2010CA 2nd REF Occurs > 1 2300 AMT Segments Occurs > 1 2300 CRC Occurs > 1 2300 CRC Occurs > 3 Times DTP Segment Required, when CR301=RorS Invalid REF01 Segment, when NM108=MI Missing DTP segment, DTP01=330 Missing DTP Segment, where DTP01=297 - Date Last Worked Missing REF segment Missing REF segment, REF01=9F Missing REF segment, REF01=F8 Missing Required CR1 Segment Missing Required DTP Segment, DTP01=435 Missing Required DTP Segment, DTP01=453 Missing Required DTP Segment, DTP01=454 Missing Required DTP Segment, DTP01=471 PRV in loop 2000A or 2310B should be present The Mandatory DTP segment (DTP/01=472) in loop 2400, was not found When CLM11 present, DTP01=439 must be present

2370 error

This section lists the description, cause, and action to take regarding the 2370 compliance map error.

- Description. Invalid loop.
- Cause. Violation of gray box rules as described in the HIPAA Implementation Guide.
- Action. Change incoming data or instruct the submitter of the data to provide a value in the field.

Map	Example of text error messages for error code 2370
270	2000C Invalid HL Loop 2000D Invalid HL Loop Missing Loop 2110C
271	Not applicable

Map	Example of text error messages for error code 2370
276	Invalid use or HL segment
277	Invalid use or HL segment
278RQ	Not applicable
278RP	Not applicable
820	Not applicable
834	Not applicable
835	Not applicable
837D	1st Loop Iteration, NM101='DN' 1st Loop Iteration, NM101='DN' 2010AA Loop Occurs > 1 2010AA Billing Prov Loop Miss 2010AB Loop Occurs > 1 2010BA Loop Occurs > 1 2010BB Loop Occurs > 1 2010BB Missing Mandatory Loop 201BC Loop Occurs > 1 2310A Loop Occurs > 2 Times 2310C Loop Occurs > 1 Times 2330A Loop Occurs > 1 Time 2330B Loop Occurs > 1 Time 2330C Loop Occurs > 1 Times 2330D Loop Occurs > 1 Time 2330E Loop Occurs > 1 Time 2420A Loop Occurs > 1 Time 2420B Loop Occurs > 1 Time 2nd Loop Iteration, NM101='P3' 2nd Loop Iteration, NM101='P3' HL04 Invalid Loop Value NM101=40 Exceed Max Occur NM101=41 Exceed max Occur
837I	2000C Invalid HL Loop 2330A Missing Required Loop LOOP ID - 2400 LX Required

Map	Example of text error messages for error code 2370
837P	1000A NM101=40 Occurs > 1 1000B NM101=41 Occurs > 1 2000A NM101=85 Occurs > 1 2000AB :NM101=87 Occurs > 1 2000BA Missing Subscriber NM1 2010BA NM101=IL Occurs > 1 2010BB NM101=PR Occurs > 1 2010BC NM101=QD Occurs > 1 2010BD NM101=AO Occurs > 1 2010CA NM101=QC Occurs > 1 LX Segment Missing

4567 error

This section lists the description, cause, and action to take regarding the 4567 compliance map error.

- Description. Required data element missing.
- Cause. Information on a required element within a segment is missing in the inbound data.
- Action. Add element information in the specified location of the segment.

Map	Example of text error messages for error code 4567
270	PER04 is missing, or not Numeric PER06 is missing, or not Numeric PER08 is missing, or not Numeric Required Data Element Missing Required PER03 element missing Required PER05 element missing Required PER07 element missing
271	Missing or mismatched LE segment Missing or mismatched LS segment Required Data Element Missing
276	Required Data Element Missing
277	Required Data Element Missing

Map	Example of text error messages for error code 4567
278RQ	2000C HI elements not consecutive 2000C TRN segment required 2000D HI elements not consecutive 2000D TRN segment required 2000F HI elements not consecutive 2010A NM1 Mandatory segment missing 2010B NM1 Mandatory segment missing 2010C NM1 Mandatory segment missing 2010E Both NM103 and NM109 cannot be NULL 2010E NM1 Mandatory segment missing A TRN segment is required in each Service loop when the requ CR6 -Invalid or Missing HI0101 CR6 requires 2000C or 2000D HI0104 CR6 requires a 2000C HI or 2000D HI segment NM108, NM109 must both be present or not included Required Data Element Missing When UM01=HS and NM108/NM109=blank, PRV is required When UM01=SC and NM108/NM109=blank, PRV is needed
278RP	2000A HL Mandatory segment missing 2000B HL Mandatory segment missing 2000C HI elements not consecutive 2000C HL Mandatory segment missing 2000C PWK05 & 06 must both be present or blank 2000C PWK05 is required when PWK02 is not 'VO' 2000D HI elements not consecutive 2000E HL Mandatory segment missing 2000F HI elements not consecutive 2000F HL Mandatory segment missing 2010D NM108, NM109 must both be present or not included 2010E Both NM103 and NM109 cannot be NULL 2010E NM108, NM109 must both be present or not included A 2000C PWK segment is invalid when a 2000D level is present A 2000CB NM1 segment is invalid when a 2000D level is present Required Data Element Missing
820	Required Data Element Missing

Map	Example of text error messages for error code 4567
834	Missing Mandatory 2000 REF01=0F Required Data Element Missing
835	2102.NM104 is required 2110 Service level DTM segment required when 2100 Claim DTM BPR11 is required when BPR04 = ACH CLP05 Amount does not equal the sum of CAS amounts where CASHDR BPR05 is required HDR.BPR07 is required HDR.BPR08 is required HDR.BPR09 is required HDR.BPR10 is required HDR.BPR12 is required HDR.BPR13 is required HDR.BPR14 is required HDR.BPR15 is required Mandatory 2100 NM1 Patient Name Required Data Element Missing SCV03 is required SVC_0101 cannot equal SVC_0601 SVC_05 cannot equal SVC_07 TS3 required if TS2 present When CLP06 is MA or MB a 2110 level DTM segment is required When CLP06 is MB, LX01 must equal 0 or 1
837D	Required Data Element Missing
837I	2300Z Missing Mandatory HI Invalid Amount Required Data Element Missing
837P	2010AA Missing Mandatory NM101 2400E DTP Service Date prior to Jan 1 2000 is missing required CR212 Required Data Element Missing When PAT08 is used, data is required in PAT07

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W