CAQH CORE Claim Status
CORE Certification Test Suite Version CS.2.0
April 2022

Revision History for Claim Status CAQH CORE Certification Test Suite

Version	Revision	Description	Date
2.0.0	Major	Phase II CORE Certification Test Suite balloted and approved by the CAQH CORE Voting Process.	July 2008
2.1.0	Major	Revised to support v5010	March 2011
CS1.0	Minor	• Non-substantive adjustments to support re-organization of operating rules into rule sets organized by business transaction (e.g., Eligibility & Benefits, Claim Status, etc.) rather than phase (e.g., Phase I, II, etc.) as approved by the CAQH CORE Board in 2019. • Operating rule naming, versioning and numbering methodologies updated to align with business transaction-based rule sets.	May 2020
CS2.0	Major	• Aligned Test Scenarios to address CAQH CORE Infrastructure Rule updates (e.g., System Availability, Connectivity, and Companion Guide requirements).	April 2022

Table of Contents

1. Introduction to Claim Status CAQH CORE Certification Test Suite

1.1. Purpose of this Document

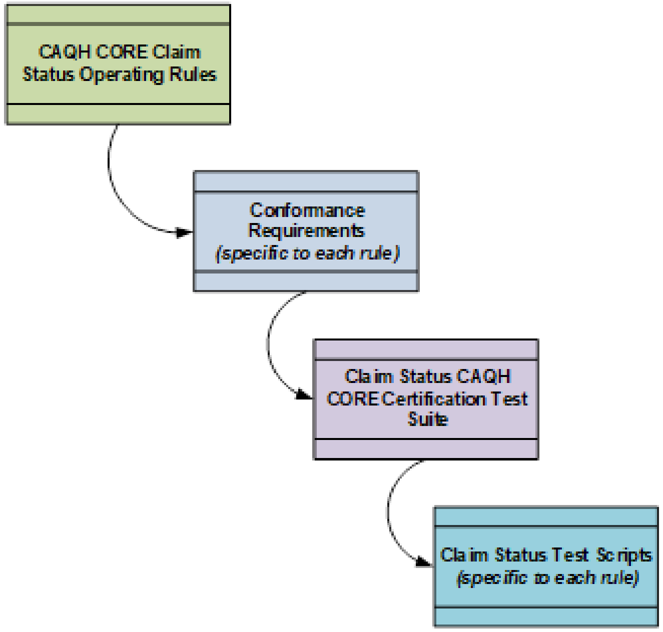
This CAQH CORE Certification Test Suite document contains all of the requirements that must be met in order for an entity seeking Claim Status CORE Certification to be awarded a Claim Status CORE Certification Seal. As such, this CAQH CORE Certification Test Suite includes:

- Two Master Scenarios describing the end-to-end claim status inquiry process in non-technical language (see §2.2).
- The specific conformance requirements and detailed testing for each CAQH CORE Claim Status (276/277) Infrastructure Rule (see §1.3, §1.4 and §3).
- The required CORE Certification Testing for each Rule, including specific detailed step-by-step test scripts by rule (see §1.5 and §3 for each rule-specific testing requirements).
- Guidance to help stakeholders better understand the various types of stakeholders to which the CAQH CORE Claim Status Operating Rules apply and how to determine when a specific rule detailed test script applies is also included (see §1.4).

Note the CAQH CORE Guiding Principles apply to the entire set of rules, including the CAQH CORE Certification Test Suite. CORE Certification Testing is not exhaustive and does not use production-level testing.

The figure below depicts the high-level parts of the testing process:

Key Components of Claim Status CORE Certification Testing


CAQH CORE Claim Status Operating Rules
Conformance Requirements (specific to each rule)
Claim Status CAQH CORE Certification Test Suite
Claim Status Test Scripts (specific to each rule)

2. Applicability of This Document

The CAQH CORE Certification Test Suite must be used by all stakeholders undergoing Claim Status CORE Certification Testing. This is required in order to maintain standard and consistent test results and CAQH CORE Claim Status Operating Rule compliance. There are no exceptions to this requirement.

2.1. The Master Scenarios

The Claim Status CAQH CORE Certification Test Suite uses two Master Scenarios (§2) to describe both the real time and batch business processes for end-to-end claim status inquiries using business language, not technical specifications to the extent appropriate.

- Master Scenario #1: Claim Status Single/Dual Clearinghouse Provider-to-Health Plan Model
- Master Scenario #2: Claim Status Provider Direct to Health Plan Model

The overall business process for a claim status inquiry does not change from a business viewpoint for each claim status operating rule. Rather, each claim status operating rule addresses a critical interoperability activity/task within the common business process.

Using only two Master Scenarios for all rules simplifies rule test scenario development since the key variables for each rule will be only the actual conformance language of the rule and then each test scenario's test objectives, assumptions, and detailed step-by-step test scripts.

2.2. Structure of Test Scenarios for all Rules

Each test scenario for each rule contains the following sections:

- Key Rule Requirements (the CAQH CORE Claim Status (276/277) Infrastructure Rule document contains the actual rule language and is the final authority for all rule requirements)
- CORE Certification conformance requirements by rule
- Test assumptions by rule
- Detailed step-by-step test scripts addressing each conformance requirement by rule for each stakeholder to which the test script applies

Each stakeholder may indicate that a specific test script does not apply to it and is required to provide a rationale for indicating a specific test script is not applicable.

2.3. Detailed Step-by-Step Test Scripts

2.3.1. Stakeholder Categories −Determining Test Script Applicability

The Detailed Step-by-Step Test Scripts for each rule specify for which stakeholder type each test script applies. The stakeholder categories are:

- Provider
- Health Plan
- Clearinghouse
- Vendor

Oftentimes Providers and Health Plans outsource various functions to Clearinghouses. In such cases a specific Clearinghouse may be acting on behalf of either a Provider stakeholder or a Health Plan stakeholder. Thus, when establishing a CORE Certification Test Profile with a CAQH CORE-authorized Testing Vendor, a Clearinghouse may be asked to indicate if it is a Provider/Clearinghouse or a Health Plan/Clearinghouse. When a Provider/Clearinghouse role is selected, the

Detailed Step-by-Step Test Scripts applicable to a Provider will apply to a Provider/Clearinghouse. Similarly, when a Health Plan/Clearinghouse role is selected, the Detailed Step-by-Step Test Scripts applicable to a Health Plan will apply to a Health Plan/Clearinghouse.

Vendor stakeholders must certify each specific product separately. Thus, when establishing a CORE Certification Test Profile with a CAQH CORE-authorized Testing Vendor you will be given the option to indicate if the product you are certifying is a Provider/Vendor product or a Health Plan/Vendor product. The Detailed Step-by-Step Test Scripts applicable to a Provider will apply to a Provider/Vendor product. Similarly, when you are certifying a Health Plan product the Detailed Step-by-Step Test Scripts applicable to a Health Plan will apply to a Health Plan/Vendor product.

2.3.2. Guidance for Health Plans Seeking Claim Status CORE Certification Who Work With a Claim Status CORE-certified Clearinghouse

Health plans seeking Claim Status CORE Certification that use a clearinghouse to send back claim status responses to providers, and to claim status inquiries from providers, may have some unique Claim Status CORE Certification issues. Because there is a clearinghouse, or similar type of intermediary, between the health plan's claim status system and the provider's claim status system, the clearinghouse will act as a "proxy" for some of the Claim Status CORE Certification requirements outlined in the Claim Status CAQH CORE Certification Test Suite. Therefore, dependent upon the scenario between the health plan and clearinghouse, the health plan may not have to undergo certification testing for some of the rules, but rather may choose the N/A option for testing for a rule, and then upload a rationale statement explaining the situation to the CAQH CORE-authorized Testing Vendor.

Reminder: ***There exist varying scenarios for this type of situation. The requirements for meeting the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements for clearinghouses and health plans differ by situation, as such variability is dependent on how the health plan interacts with the clearinghouse and what services (i.e., functions and capabilities) the clearinghouse provides to the health plan. Therefore, please keep in mind that certification testing will differ by scenario.***

2.3.3. Guidance for Providers Seeking Claim Status CORE Certification Who Work With a Claim Status CORE-certified Clearinghouse

Provider organizations seeking Claim Status CORE Certification that use a clearinghouse to send claim status requests to payers, and to receive claim status responses from payers, may have some unique Claim Status CORE Certification issues. Because there is a clearinghouse, or similar type of intermediary, between the provider's claim status system and the payer's claim status system, the clearinghouse will act as a "proxy" for some of the Claim Status CORE Certification requirements outlined in the Claim Status CAQH CORE Certification Test Suite. Therefore, dependent upon the scenario between the provider and clearinghouse, the provider may not have to undergo certification testing for some of the rules, but rather may choose the N/A option for testing for a rule, and then upload a rationale statement explaining the situation to the CORE-authorized testing vendor.

Reminder: There exist varying scenarios for this type of situation. The requirements for meeting the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements for clearinghouses and providers differ by situation, as such variability is dependent on how the provider interacts with the clearinghouse and what services (i.e., functions and capabilities) the clearinghouse provides to the provider. Therefore, please keep in mind that certification testing will differ by scenario.

3. Claim Status Master Scenarios

3.1. Purpose of the Business Process Scenarios

The business process scenarios described for claims status request for real-time and batch depict the workflows and information flows that support an efficient management process for health plans and providers. The CAQH CORE Claim Status Operating Rules for claim status request are designed to support these business processes and their technical components. The CAQH CORE Claim Status Operating Rules should promote increased health plan service level performance, stimulate vendors to enhance their products to support claims status request management and encourage providers to utilize these transactions.

These scenarios serve several purposes, including identifying and confirming the placement in the workflow in the provider setting and health plan setting where the following transformations occur:

- Collecting the information to initiate claim status request in the provider's workplace and identifying the individual or role where this takes place.
- The system or mechanism used to create and manage the EDI interchange outbound and inbound from the provider.
- Identify the work and information flows at the health plan upon receiving and validating the claims request transaction.
- Describe the information process at the health plan, including files and databases to be used to collect the information and prepare the response to the claims status request.
- The process to prepare and send the claims status response EDI transaction from the health plan.
- The process at the provider of receiving the claims status response EDI transaction and preparing it for use.
- The identification of the information presentation(s) used at the provider organization to process the information in the claims status response to be used in determining what action to take and by whom within the organization.

It is important to understand each of these touch points as well as the role of one or more clearinghouses between the two trading partners in order to develop the details of the rules, the CORE Certification and testing process, the test data, and as a guide toward implementation for the parties involved.

The business processes are vendor neutral, with an understanding that the details about how the work processes are conducted within information systems and are used by members of the workforce will vary depending on the vendor products utilized. Note that in some cases, a provider's clearinghouse may provide some of the functionality described as a provider role in these scenarios. That is a business decision to be made between the provider and its clearinghouse. Likewise, the health plan's clearinghouse may provider some of the functional capabilities for the health plan. Again, this is a business decision between the health plan and the health plan's clearinghouse.

3.1.1. Current and Future Workflow and Information Flow Processes

Currently in many settings, claims status request process is not well integrated into the business processes of healthcare providers. As a result, many providers are not realizing the benefits of administrative simplification through an automated workflow and process for claim status inquiries. For those providers already using the claim status request transactions, the CAQH CORE Claim Status (276/277) Infrastructure Rules improve performance with a greater availability of health plan systems and more consistent/predictable response times to receive claim status request responses. Some providers ignore the process and resubmit claims when they are not adjudicated within a normal or expected timeframe. Other providers ignore the claims status request function and trust that the health plan has received their claim and that eventually it will be adjudicated. Some providers call health plans with their inquiries about claim status. None of these approaches are designed to provide an efficient, integrated business process for providers and health plans to exchange information on the status of claims that are "overdue."

In some cases, there are vendor products with management tools to support an automated claims status request. However, most vendor products (practice management systems and hospital information systems) either do not have management tools to efficiently support this process, or providers choose not to use them or license them when they do exist. Instead, telephone calls and resubmitted overdue claims are commonly used, both of which consume resources for both the provider and the health plan.

3.1.2. Single/Dual Clearinghouse Provider-to-Health Plan Business Model

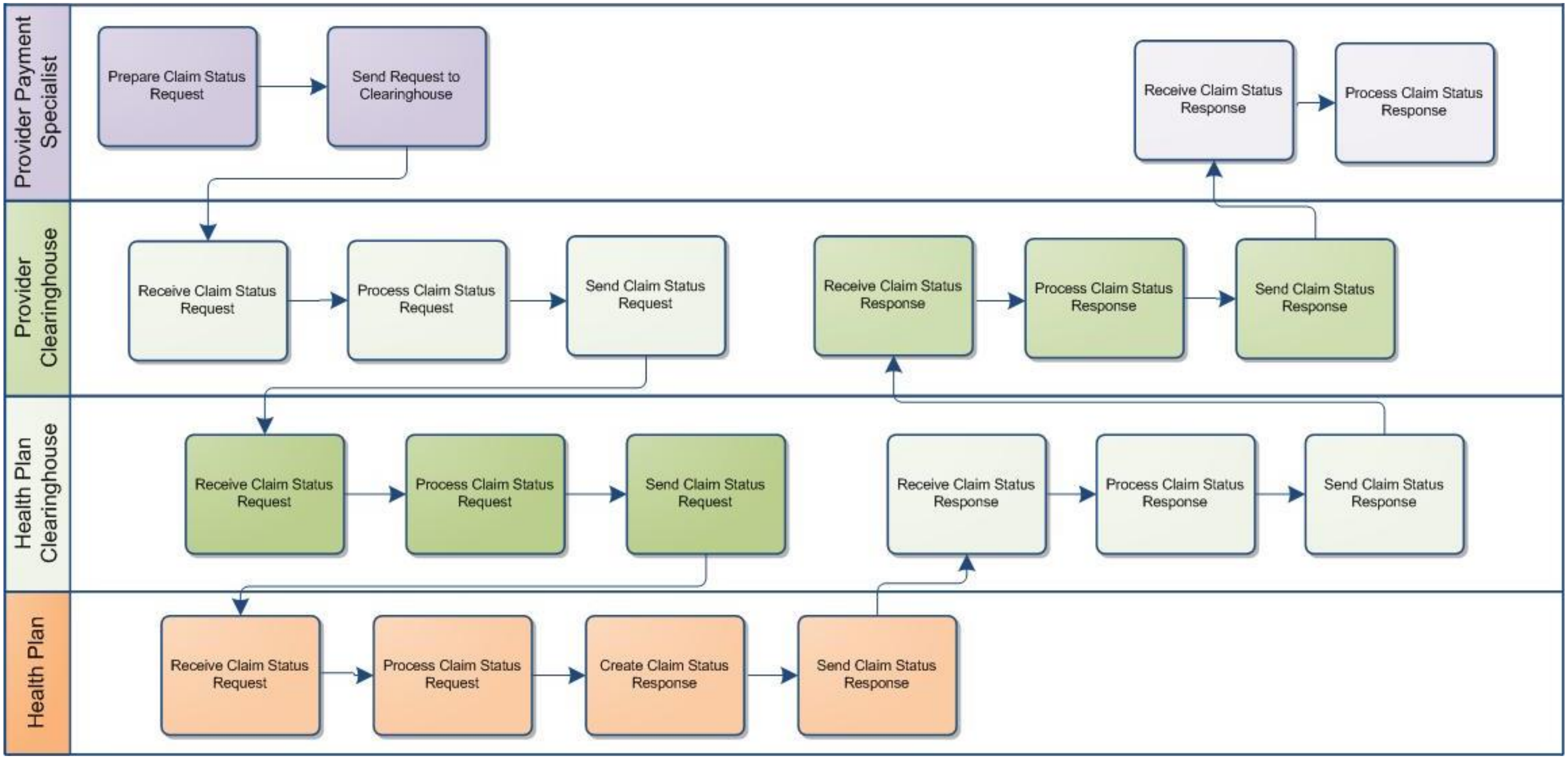
3.1.2.1. Introduction

This CORE Master Business Process Scenario describes real time and batch business processes for end-to-end insurance claim status inquiries using business language, not technical specifications to the extent appropriate, in which there are either one or two clearinghouses providing services to the healthcare provider and health plan or information source. Since the overall business process for insurance claim status request does not fundamentally change from a business viewpoint, each CAQH CORE Claim Status (276/277) Infrastructure Rule addresses a critical interoperability activity/task within the common business process. Thus, the focus for this scenario is on the EDI aspects of the overall end-to-end business process and not on attempting to describe all of the activities and tasks typically performed by each of the stakeholders in the process.

3.1.2.2. Background

This scenario describes the healthcare insurance claim status request end-to-end business process and the key activities and tasks conducted between a healthcare provider and a health plan where each party uses the services of a healthcare clearinghouse. For purposes of CORE Certification Testing, stakeholders include providers, health plans, clearinghouses, switches, other intermediaries, and solution vendors. The end-to-end information flow is the same whether the claim status request is conducted in real time or batch. It is the CAQH CORE Claim Status (276/277) Infrastructure Rules specify the respective response times for real time and for batch processing modes. Figure 1 below depicts this overall information flow.

Figure 1: Claim Status Process: Single/Dual Clearinghouse Provider-to-Health Plan Model


Provider Payment Specialist
Prepare Claim Status Request
Send Request to Clearinghouse
Receive Claim Status Response
Process Claim Status Response
Provider Clearinghouse
Receive Claim Status Request
Process Claim Status Request
Send Claim Status Request
Receive Claim Status Response
Process Claim Status Response
Send Claim Status Response
Health Plan Clearinghouse
Receive Claim Status Request
Process Claim Status Request
Send Claim Status Request
Receive Claim Status Response
Process Claim Status Response
Send Claim Status Response
Health Plan
Receive Claim Status Request
Process Claim Status Request
Create Claim Status Response
Send Claim Status Response

Each stakeholder type is equipped with an automated system (the “system”) appropriate to its needs, e.g., a provider would have a hospital (or health) information system, commonly referred to as an HIS, or an automated practice management system (the “system”), commonly referred to as a PMS.

The “system” is defined as all of the components necessary for the stakeholder to conduct its automated business processes, e.g., all necessary network nodes, all platform components delivered by the vendor, and all the vendor components (e.g. documentation) included with the system. The system may consist of one or many workstations, servers and mainframe systems, and usually supports payment collection in the business office at the workstation if the stakeholder is a provider.

3.1.2.3. Claim Status Request Business Process Description

Business Office Claim Payment Management

A business office insurance payment specialist at the provider's office is inquiring about a claim that has been submitted, for which the status of adjudication is unknown. The business office insurance payment specialist collects the required data from the "system", following prompts on the workstation and enters all of the necessary information into the PMS/HIS. In some systems, the request may be initiated automatically based on a past due expected date for adjudication reporting.

When all of the necessary patient demographic and insurance information is entered, the payment specialist is prompted to submit a claim status request transaction by either a menu selection or by clicking an icon (as determined by the PMS/HIS vendor user interface design).

The PMS/HIS automatically edits the claim status transaction for completeness and valid data values where applicable and prompts the payment specialist to correct any invalid or omitted data. When the transaction editing is completed, the PMS/HIS assigns a unique internal tracking number, records the identification and address of the workstation used by the payment specialist, and creates the claim status request transaction.

Using internal tables/files, the PMS/HIS determines the Internet address for its clearinghouse, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the claim status request transaction, and establishes a communications session with the clearinghouse's system. The claim status request transaction created by the PMS/HIS for transfer to its clearinghouse/switch may be either in a proprietary format or a fully enveloped X12 Interchange containing the v5010 276 claim status request transaction set.

Provider Clearinghouse Real Time Claim Status Request Process

The clearinghouse's Internet portal accepts the provider's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the claim status request transaction, which is then extracted and passed to the appropriate systems in the clearinghouse for further processing. The clearinghouse's system edits the claim status transaction for completeness and valid data values where applicable. If the claim status transaction fails editing, the clearinghouse returns to the provider an appropriate error message or acknowledgement describing the reasons for failure and rejection, thereby allowing the provider to correct and re-submit the claim status transaction. Such error message or acknowledgement may be either a proprietary or valid X12 Acknowledgement, depending on the type and range of services the clearinghouse is providing.

Using internal tables/files and/or an external directory service, the clearinghouse system determines the Internet address for the clearinghouse serving the health plan specified in the provider's claim status request transaction, creates and envelopes the complete X12 Interchange containing the v5010 276 request, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the V5010 X12 276 Interchange, and establishes a communications session with the health plan's clearinghouse. Depending on the range and type of services being provided to the provider by the clearinghouse, the clearinghouse may or may not have responsibility for creating the correct X12 Interchange containing the v5010 276 Claim status request or for performing other data validation/transformation and/or editing functions prior to forwarding the claim status request to either the health plan or the health plan's clearinghouse. Upon successful transfer of the V5010 X12/276 Interchange to the health plan's clearinghouse, the provider's clearinghouse maintains the communications session open and active until receipt of either a V5010 X12 999 or V5010 X12 277 Interchange from the health plan's clearinghouse.[1]

If the V5010 X12 276 Interchange fails X12 TR3 implementation guide verification at the health plan's clearinghouse, the provider's clearinghouse receives the V5010 X12/999 Implementation Acknowledgement indicating the rejection of the Functional Group, extracts/reformats the rejection acknowledgement and takes appropriate action to resolve the rejection. This may be by returning it to the provider's PMS/HIS or correcting the errors within the clearinghouse.

[1] Alternatively, a single clearinghouse may be serving both the provider and the health plan to which the claims status request transaction is to be transmitted. In this case, the single clearinghouse would not only perform the reformatting of non-standard data and non-standard format received from the provider into the HIPAA-adopted standard, but would then perform the reformatting of the standard data and standard format into non-standard data and non-standard format required by the health plan. A similar set of functions would be performed when processing the claims status response transaction received from the health plan. See Health Plan Clearinghouse Real Time Claim Status Request Process section in this document for a complete description of this process.

When the V5010 X12 277 claim status response transaction is received from the health plan's clearinghouse, the clearinghouse's Internet portal records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 277 Interchange, returns a signal to the health plan's clearinghouse that the V5010 X12 277 Interchange payload has been successfully stored into persistent storage, and passes the V5010 X12 277 Interchange to the clearinghouse's EDI management system for further processing. The clearinghouse's EDI management system processes (validates) the V5010 X12 277 Interchange which contains the requested claim status data. The EDI management system extracts the v5010 277 response data, creates the required claim status response transaction required by the provider's PMS/HIS (may be either a proprietary or valid V5010 X12 277 Interchange), and transfers the claim status response transaction to the provider's PMS/HIS.

Health Plan Clearinghouse Real Time Claim Status Request Process

The health plan's clearinghouse Internet portal accepts the provider's clearinghouse's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 276 Interchange, returns a signal to the provider's clearinghouse that the V5010 X12 276 Interchange payload has been successfully stored into persistent storage, and passes the V5010 X12 276 Interchange to the clearinghouse's EDI management system for further processing. The clearinghouse's EDI management system, processes (validates) the V5010 X12 276 Interchange.

If the V5010 X12 276 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the EDI management system extracts the claim status request data from the v5010 276 transaction set, creates the required internal claim status request transaction required by the health plan. Using internal tables/files and/or an external directory service, the clearinghouse system determines the Internet address for the health plan specified in the provider's claim status request transaction, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the claim status request transaction, and establishes a communications session with the health plan if such a communications link is not already open and active. Upon successful transfer of the claim status request transaction to the health plan, the clearinghouse maintains the communication session open and active pending receipt of the claim status response transaction from the health plan.

If the v5010 X12 276 Interchange fails X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, returns the rejection acknowledgement to the provider's clearinghouse, terminates the communications session (if necessary) and discontinues any further processing of the claim status request transaction.

When the claim status response transaction is received from the health plan, the clearinghouse's EDI management system edits the claim status response data for correctness and completeness, creates the X12 Interchange containing the v5010 277 claim status response, passes the V5010 X12 277 Interchange to the open communications session which returns the V5010 X12 277 Interchange to the provider's clearinghouse.

Health Plan Real Time Claim Status Request Process

The health plan's Internet portal accepts the clearinghouse's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the claim status request transaction, which is then extracted and passed to the health plan's claim status request system for processing. The claim status system accesses all of the necessary internal data stores (files, databases, etc.) to process the claim status request transaction to determine the status of the claim identified in the request. The data are then assembled and routed to the health plan's clearinghouse. When the clearinghouse signals successful receipt of the claim status response transaction to the health plan's system, the communications session may be terminated or maintained open and active as determined between the health plan and its clearinghouse.

Provider Real Time Claim Status Response Process

The provider's PMS/HIS receives the claim status response transaction from its clearinghouse, records the message receipt date/time, assigns an internal tracking number to the message linked to the claim status response transaction, and matches the tracking number, message receipt date/time to the corresponding claim status request transaction. The PMS/HIS then processes (validates) the claim status response transaction, which is routed to the correct workstation for display to the payment specialist.

The PMS/HIS displays the claim status information, enabling the payment specialist to take appropriate action by obtaining corrected claim data as indicated from the PMS/HIS or other sources and either resubmitting a corrected claim status request or a corrected claim.

If the claim status response transaction contains the requested information, the PMS/HIS displays the claim status information, enabling the payment specialist to confirm the claim status. Status of the claim within the health plan's adjudication process may include pre-adjudication acceptance/rejection, incorrect or incomplete claim pended, claim suspended/additional information is being requested, or claim finalized. Subsequent activities may include calling the patient or health plan, or pending further action to a later date. The claim status information as represented by the status and category codes received in the v5010 271 response and the date of the request are stored in the PMS/HIS.

Provider Batch Claim Status Process

On a daily basis the provider's PMS/HIS automatically scans all past due claim adjudication responses for the current date, extracts all of the necessary data, creates one or more batches of claim status inquiries for each health plan covering the overdue adjudication responses for that date, assigns unique internal tracking numbers and records the date/time for each batch.

Using internal tables/files and/or an external directory service, the PMS/HIS determines the Internet address for each health plan, envelopes the complete X12 Interchange containing the batch of v5010 276 inquiries for each health plan, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the correct batch V5010 X12 276 Interchange, establishes a communications session with each health plan's system and transfers the batch of claim status request transactions in either a proprietary non-standard format or V5010 X12 276 Interchange to its clearinghouse for transmission to the health plan's clearinghouse prior to 9:00 pm ET, the daily cut-off time for batch submissions.

Provider Clearinghouse Batch Claim Status Request Process

The clearinghouse's Internet portal accepts the provider's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the claim status request transaction, which is then extracted and passed to the appropriate systems in the clearinghouse for further processing. The clearinghouse's system edits the claim status transaction for completeness and valid data values where applicable. If the claim status transaction fails editing, the clearinghouse returns to the provider an appropriate error message or acknowledgement describing the reasons for failure and rejection, thereby allowing the provider to correct and re-submit the claim status transaction. Such error message or acknowledgement may be either a proprietary or valid X12 Acknowledgement, depending on the type and range of services the clearinghouse is providing.

Using internal tables/files and/or an external directory service, the clearinghouse system determines the Internet address for the clearinghouse serving the health plan specified in the provider's claim status request transaction, creates and envelopes the complete X12 Interchange containing the v5010 276 request, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the V5010 X12 276 Interchange, and establishes a communications session with the health plan's clearinghouse. Depending on the range and type of services being provided to the provider by the clearinghouse, the clearinghouse may or may not have responsibility for creating the correct X12 Interchange containing the v5010 276 Claim Status Request or for performing other data validation/transformation and/or editing functions prior to forwarding the claim status request to either the health plan or the health plan's clearinghouse. Upon successful transfer of the V5010 X12/276 Interchange to the health plan's clearinghouse, the provider's clearinghouse either terminates the session (if necessary) or maintains the communications session open and active until receipt of either a V5010 X12 999 or V5010 X12 277 Interchange from the health plan's clearinghouse.

If the V5010 X12 276 Interchange fails X12 TR3 implementation guide verification at the health plan's clearinghouse, the provider's clearinghouse receives the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, extracts/reformats the rejection acknowledgement and takes appropriate action to resolve the rejection. This may be by returning it to the provider's PMS/HIS or correcting the errors within the clearinghouse.

When the V5010 X12 277 claim status response transaction is received from the health plan's clearinghouse, the clearinghouse's Internet portal records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 277 Interchange, returns a signal to the health plan's clearinghouse that the V5010 X12 277 Interchange payload has been successfully stored into persistent storage, and passes the V5010 X12 277 Interchange to the clearinghouse's EDI management system for further processing. The clearinghouse's EDI management system processes (validates) the V5010 X12 277 Interchange which contains the requested claim status data. The EDI management system extracts the v5010 277 response data, creates the required claim status response transaction required by the provider's PMS/HIS (may be either a proprietary or valid V5010 X12 277 Interchange), and transfers the claim status response transaction to the provider's PMS/HIS.

Health Plan Clearinghouse Batch Claim Status Request Process

The health plan's clearinghouse Internet portal accepts the provider's clearinghouse's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 276 Interchange, returns a signal to the provider's clearinghouse that the V5010 X12 276 Interchange payload has been successfully stored into persistent storage, and passes the V5010 X12 276 Interchange to the clearinghouse's EDI management system for further processing. The clearinghouse's EDI management system, processes (validates) the V5010 X12 276 Interchange.

If the V5010 X12 276 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating acceptance of the V5010 X12 276 Interchange, returns the V5010 X12 999 Interchange to the provider's clearinghouse, extracts the claim status request data from the v5010 276 transaction set, and creates the required internal claim status request transactions required by the health plan.

Using internal tables/files and/or an external directory service, the clearinghouse system determines the Internet address for the health plan specified in the provider's claim status request transaction, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the claim status request transaction, and establishes a communications session with the health plan if such a communications link is not already open and active. Upon successful transfer of the claim status request transactions to the health plan, the clearinghouse either terminates (if necessary) or maintains the communication session open and active pending receipt of the claim status response transactions from the health plan.

If the v5010 X12 276 Interchange fails X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, returns the rejection acknowledgement to the provider's clearinghouse, terminates the communications session (if necessary) and discontinues any further processing of the request transaction.

When the claim status response transactions are received from the health plan, the clearinghouse's EDI management system edits the claim status response data for correctness and completeness, creates the X12 Interchange containing the v5010 277 claim status responses, passes (with or without errors) the V5010 X12 277 Interchange to the communications module which returns the V5010 X12 277 Interchange to the provider's clearinghouse. The clearinghouse's EDI management system processes (validates) the V5010 X12 277 Interchange which contains the requested claim status data.

Health Plan Batch Claim Status Request Process

The health plan's Internet portal accepts the provider's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the batch V5010 X12 276 Interchange, which is then extracted and passed to the health plan's EDI management system for further processing. The health plan's Internet portal returns the correct HTTP message accepted code to the provider's PMS/HIS and terminates the communications session.

The health plan's EDI management system, processes (validates) the batch V5010 X12 276 Interchange. If the batch V5010 X12 276 Interchange fails X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, stages the acknowledgement for subsequent retrieval by the provider's clearinghouse, and discontinues any further processing of the batch V5010 X12 276 Interchange.

If the batch v5010 X12 276 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the acceptance of the v5010 X12 276 Functional Group, and stages the acknowledgement for subsequent retrieval by the provider's PMS/HIS.

The EDI management system extracts the claim status request data from the v5010 276 transaction set, creates the required internal request transaction(s) which are routed to the claim status system for processing. The claim status system accesses all of the necessary internal data stores (files, databases, etc.) to process the claim status inquiries to determine the claim status for each of the inquiries. The data are then assembled and routed to the health plan's EDI management system.

The EDI management system edits the claim status response data for correctness and completeness, creates the batch(es) X12 Interchange containing the v5010 277 claim status responses, stages the batch(es) V5010 X12 277 Interchange for subsequent retrieval by the provider's PMS/HIS.

Provider's Batch Claim Status Response Process

Two hours after transferring the batch V5010 X12 276 Interchange to its clearinghouse, the provider's PMS/HIS establishes a communications session with its clearinghouse, requests either a list of available files for retrieval or specific file(s). Specific file(s) may be either an V5010 X12 999 Interchange, or an V5010 X12 277 Interchange or any combination of these. The clearinghouse responds appropriately to the provider's PMS/HIS request. The provider's PMS/HIS then retrieves the requested and/or available file(s), records the message receipt date/time, assigns internal tracking number(s) to the message and retrieved file(s) linked to the X12 Interchange(s), and matches the tracking number, message receipt date/time to the corresponding V5010 X12 276 Interchange. The PMS/HIS then processes (validates) the X12 Interchange(s) retrieved.

If the batch V5010 X12 277 Interchange fails X12 TR3 implementation guide verification, the PMS/HIS generates the V5010 X12 999 Implementation Acknowledgement, establishes a communication session with the clearinghouse and transfers the V5010 X12 999 to the clearinghouse. The PMS/HIS also generates a notice to the provider's appropriate internal support staff for any problem resolution following established internal procedures.

The PMS/HIS extracts the claim status response data from the v5010 277 transaction set, creates the required internal claim status response transaction(s) which are routed to the correct workstation for analysis and processing by the designated support staff.

The PMS/HIS displays the claim status information, enabling the payment specialist to take appropriate action by obtaining co rrected claim data as indicated from the PMS/HIS or other sources and either resubmitting a corrected claim status request or a corrected claim.

If the v5010 277 claim status response transaction contains the requested claim status information, the PMS/HIS displays the information, enabling the payment specialist staff to extend the expected adjudication date, contact the patient, or contact the health plan by telephone, fax or other means to resolve problems associated with completing adjudication.

3.1.3. Provider Direct-to-Health Plan Business Model

3.1.3.1. Introduction

This CORE Master Business Process Scenario describes real time and batch business processes for end-to-end insurance verification/claim status inquiries using business language, not technical specifications to the extent appropriate, in which the healthcare provider submits inquiries directly to the health plan or information source without using the services of a clearinghouse or other intermediary. Since the overall business process fo r insurance verification/claim status request does not fundamentally change from a business viewpoint, each CAQH CORE Claim Status (276/277) Infrastructure Rule addresses a critical interoperability activity/task within the common business process. Thus, the focus for this scenario is on the EDI aspects of the overall end-to-end business process and not on attempting to describe all of the activities and tasks typically performed by each of the stakeholders in the process.

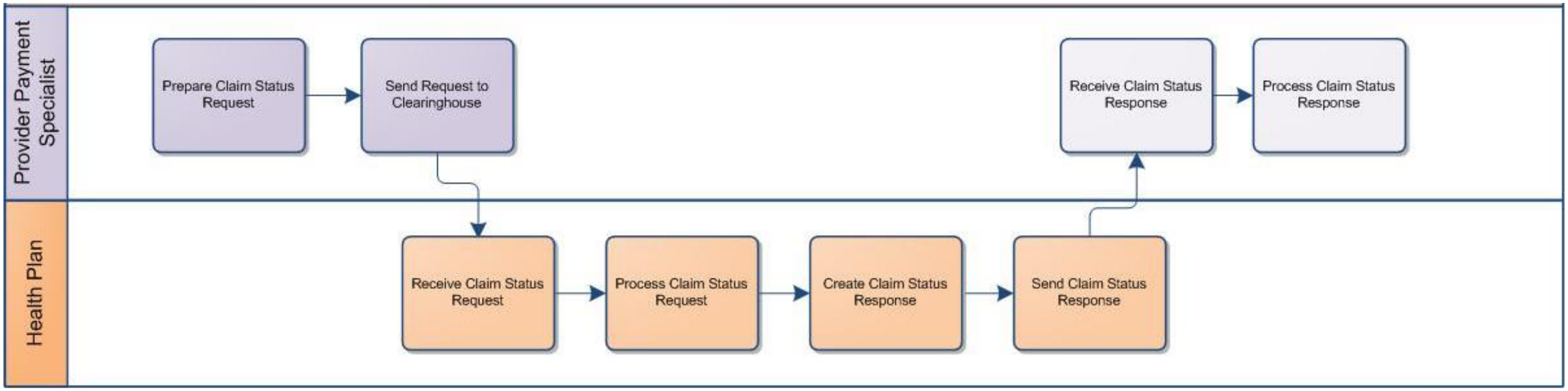
3.1.3.2. Background

This scenario describes the healthcare insurance verification/claim status end-to-end business process and the key activities and tasks conducted between a healthcare provider connecting directly to a health plan. For purposes of Claim Status CORE Certification Testing for this scenario, stakeholders include providers, health plans and solution vendors.

Each stakeholder type is equipped with an automated system (the "system") appropriate to its needs, e.g., a provider would have a hospital (or health) information system, commonly referred to as a HIS, or an automated practice management system (the "system"), commonly referred to as a PMS.

The "system" is defined as all of the components necessary for the stakeholder to conduct its automated business processes, e.g., all necessary network nodes, all platform components delivered by the vendor, and all the vendor components (e.g. documentation) included with the system. The system may consist of one or many workstations, servers and mainframe systems, and usually supports payment collection in the business office at the workstation if the stakeholder is a provider. The end-to-end information flow is the same whether the claim status request is conducted in real time or batch. It is the CAQH CORE Claim Status Operating Rules that specify the respective response times for real time and for batch processing modes. Figure 2 below depicts this overall information flow.

Figure 2: Claim Status Process: Provider Direct-to-Health Plan Model


Provider Payment Specialist
Prepare Claim Status Request
Send Request to Clearinghouse
Receive Claim Status Response
Process Claim Status Response
Health Plan
Receive Claim Status Request
Process Claim Status Request
Create Claim Status Response
Send Claim Status Response

3.1.3.3. *Claim Status Request Business Process Description*

Business Office Claim Payment Management

A business office insurance specialist at the provider's office is inquiring about a claim that has been submitted, for which adjudication and response is overdue. The business office insurance payment specialist collects the required data from the "system" following prompts on the workstation and enters all of the necessary information into the PMS/HIS. In some systems, the request may be initiated automatically based on a past due expected date f or adjudication reporting.

When all of the necessary patient demographic and insurance information is entered, the payment specialist is prompted to submit a claim status request transaction by either a menu selection or by clicking an icon (as determined by the PMS/HIS vendor user interface design.)

The PMS/HIS automatically edits the claim status transaction for completeness and valid data values where applicable and prompts the payment specialist to correct any invalid or omitted data. When the transaction editing is completed, the PMS/HIS assigns a unique internal tracking number, records the identification and address of the workstation used by the payment specialist, and creates the claim status request transaction.

Using internal tables/files and/or an external directory service, the PMS/HIS determines the Internet address for the health plan where the claim was submitted, creates and envelopes the complete X12 Interchange containing the v5010 276 request, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the V5010 X12/276 Interchange, and establishes a communications session with the health plan's system.

Health Plan Real Time Claim Status Request Process

The health plan's Internet portal accepts the provider's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 276 Interchange, which is then extracted and passed to the health plan's EDI management system for further processing. The health plan's EDI management system, processes (validates) the V5010 X12 276 Interchange.

If the V5010 X12 276 Interchange fails X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, returns the rejection acknowledgement to the provider, terminates the communications session and discontinues any further processing of the request transaction.

If the v5010 X12 276 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the EDI management system extracts the claim status request data from the v5010 276 transaction set, creates the required internal request transaction which is routed to the claim status system for processing. The claim status system accesses all of the necessary internal data stores (files, databases, etc.) to process the claim status request to determine the status of the claim identified in the request. The data are then assembled and routed to the health plan's EDI management system.

The EDI management system edits the claim status response data for correctness and completeness, creates the X12 Interchange containing the v5010 277 claim status response, passes the V5010 X12 277 Interchange to the open communications session which returns the V5010 X12 277 Interchange to the provider's PMS/HIS. The health plan's Internet portal then terminates the communications session upon successful transfer of the V5010 X12 277 Interchange to the provider's system.

Provider's Real Time Claim Status Response Process

The provider's PMS/HIS receives the V5010 X12 277 Interchange from the health plan, records the message receipt date/time, assigns an internal tracking number to the message linked to the V5010 X12 277 Interchange, and matches the tracking number, message receipt date/time to the corresponding V5010 X12 276 Interchange. The PMS/HIS then processes (validates) the V5010 X12 277 Interchange.

If the V5010 X12 277 Interchange fails X12 TR3 implementation guide verification, the PMS/HIS generates a notice to the provider's appropriate internal support staff for problem resolution following established internal procedures. No rejection acknowledgement is returned to the health plan.

If the V5010 X12 277 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the PMS/HIS extracts the claim status response data from the v5010 277 transaction set, creates the required internal claim status response transaction which is routed to the correct workstation for display to the scheduler.

The PMS/HIS displays the claim status information, enabling the payment specialist to take appropriate action by obtaining corrected claim data as indicated from the PMS/HIS or other sources and either resubmitting a corrected claim status request or a corrected claim.

If the v5010 277 claim status response transaction contains the requested information, the PMS/HIS displays the information, enabling the payment specialist to confirm the claim status. Status of the claim within the health plan's adjudication process may include pre-adjudication acceptance/rejection, incorrect or incomplete claim pended, claim suspended/additional information being requested, or claim finalized. Subsequent activities may include calling the patient or the health plan, or pending further action to a later date. Status codes and the date of the request are stored in the PMS/HIS.

Provider's Batch Claim Status Process

On a daily basis the provider's PMS/HIS automatically scans all past due claim adjudication responses for the current date, extracts all of the necessary data, creates one or more batches of claim status inquiries for each health plan covering the overdue adjudication responses for that date, assigns unique internal tracking numbers and records the date/time for each batch.

Using internal tables/files and/or an external directory service, the PMS/HIS determines the Internet address for each health plan, envelopes the complete X12 Interchange containing the batch of v5010 276 inquiries for each health plan, creates the message encapsulation envelope, assigns a payload identifier, records the date/time, links the message to the correct batch V5010 X12 276 Interchange, establishes a communications session with each health plan's system and transfers the batch V5010 X12 276 Interchange to the health plan.

Health Plan Batch Claim Status Request Process

The health plan's Internet portal accepts the provider's system logon, records the message receipt date/time, assigns an internal tracking number to the message linked to the batch V5010 X12 276 Interchange, which is then extracted and passed to the health plan's EDI management system for further processing. The health plan's Internet portal returns the correct HTTP message accepted code to the provider's PMS/HIS and terminates the communications session.

The health plan's EDI management system, processes (validates) the batch V5010 X12 276 Interchange. If the batch V5010 X12 276 Interchange fails X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the rejection of the Functional Group, stages the rejection acknowledgement for subsequent retrieval by the provider's PMS/HIS, and discontinues any further processing of the batch V5010 X12 276 Interchange.

If the batch V5010 X12 276 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the EDI management system automatically generates the V5010 X12 999 Implementation Acknowledgement indicating the acceptance of the V5010 X12 276 Functional Group, and stages the acknowledgement for subsequent retrieval by the provider's PMS/HIS.

The EDI management system extracts the claim status request data from the v5010 276 transaction set, creates the required internal request transaction(s) which are routed to the claim status system for processing. The claim status system accesses all of the necessary internal data stores (files, databases, etc.) to process the claim status inquiries to determine the claim status for each of the inquiries. The data are then assembled and routed to the health plan's EDI management system.

The EDI management system edits the claim status response data for correctness and completeness, creates the batch(es) X12 Interchange containing the v5010 277 claim status responses, stages the batch(es) V5010 X12 277 Interchange for subsequent retrieval by the provider's PMS/HIS.

Provider's Batch Claim Status Response Process

Two hours after transferring the batch V5010 X12 276 Interchange to the health plan's Internet portal, the provider's PMS/HIS establishes a communications session with each health plan's system, requests either a list of available files for retrieval or specific file(s). Specific file(s) may be either an V5010 X12 999 Implementation Acknowledgement or an V5010 X12 277 Interchange or any combination of these. The health plan's Internet portal responds appropriately to the provider's PMS/HIS request. The provider's PMS/HIS then retrieves the requested and/or available file(s), records the message receipt date/time, assigns internal tracking number(s) to the message and retrieved file(s) linked to the X12 Interchange(s), and matches the tracking number, message receipt date/time to the corresponding V5010 X12 276 Interchange. The PMS/HIS then processes (validates) the X12 Interchange(s) retrieved.

If the batch V5010 X12 277 Interchange fails X12 TR3 implementation guide verification, the PMS/HIS generates an V5010 X12 999 Implementation Acknowledgement, establishes a communication session with the appropriate health plan's Internet portal and transfers the V5010 X12 999 Implementation Acknowledgement to the health plan. The PMS/HIS also generates a notice to the provider's appropriate internal support staff for any problem resolution following established internal procedures.

If the v5010 X12 277 Interchange passes (with or without errors) X12 TR3 implementation guide verification, the PMS/HIS extracts the claim status response data from the v5010 277 transaction set, creates the required internal claim status response transaction(s) which are routed to the correct workstation for analysis and processing by the designated support staff.

The PMS/HIS displays the claim status information, enabling the payment specialist to take appropriate action by obtaining corrected claim data as indicated from the PMS/HIS or other sources and either resubmitting a corrected claim status request or a corrected claim.

If the v5010 277 claim status response transaction contains the requested claim status information, the PMS/HIS displays the information, enabling the payment specialist staff to extend the expected adjudication date, contact the patient, or contact the health plan by telephone, fax or other means to resolve problems associated with completing adjudication.

4. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Batch Acknowledgement Requirements Test Scenario

4.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Requires that

1. The receiver of a v5010 276 or a v5010 277 must always return a v5010 999 implementation acknowledgement to indicate that the Functional Group was either accepted, accepted with errors, or rejected. (§4.3.1)
2. The v5010 999 must not be returned during the initial communications session in which the v5010 276 batch is submitted. (§4.3.2)

4.2. Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Batch Acknowledgement Rule Requirement. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

1. A v5010 999 is returned to indicate either acceptance, acceptance with errors, or rejection of a Functional Group (including the enclosed Transaction Set).
    a. A v5010 999 must ALWAYS be returned whether or not there are errors in the Functional Group and enclosed Transaction Set.
2. A v5010 277 response transaction must always be returned for an Interchange, Functional Group and Transaction Set that complies with X12 TR3 implementation guide requirements.

4.3. Test Scripts Assumptions

1. All communications sessions and logon's are valid; no error conditions are created or encountered.
2. Test scripts will test ONLY for valid and invalid X12 Interchange, Functional Group, Transaction Set and will not test for v5010 277 data content.
3. Test scripts will test the following error conditions:
    a. Invalid X12 Interchange (ISA control number match error)
    b. Invalid Functional Group (GS/GE control number match error)
    c. Invalid Transaction Set (missing required segment)
4. Test scripts will test the following valid conditions:
    a. Valid X12 Interchange Control Segments
    b. Valid Functional Group Control Segments
    c. Valid X12 Transaction Set
5. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

4.4. Detailed Step-By-Step Test Script

REMINDER: CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [2]				
						Provider	**Health Plan**	**Clearinghouse**	**Vendor**	**N/A [3]**
1.	A v5010 999 is returned on an invalid Functional Group (Key Rule Requirement #1)	An X12 Interchange containing only a v5010 999		☐ Pass	☐ Fail	☒	☒	☒	☒	☐
2.	A v5010 277 response transaction is returned for a Functional Group and Transaction set that complies with the v5010 X12 TR3 implementation guide (Key Rule Requirement #1)	An X12 Interchange containing a v5010 277		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

[2] A checkmark in the box indicates the stakeholder type to which the test applies.

[3] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

5. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Real Time Acknowledgement Requirements Test Scenario

5.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Requires that

1. A v5010 999 is returned only to indicate a v5010 276 Functional Group (including the enclosed Transaction Set) error resulting in the rejection of the entire Functional Group. (§4.2.1.1)
   a. A v5010 999 must not be returned if the v5010 276 Functional Group and enclosed Transaction Set is not rejected. (§4.2.1.1)
2. A v5010 277 must always be returned for an Interchange, Functional Group and Transaction Set that complies with X12 v5010 276 requirements. (§4.2.1.2)

5.2. Conformance Testing Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

These scenarios test the following conformance requirements of the CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Real Time Acknowledgement Requirements. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

1. A v5010 999 is returned only to indicate a Functional Group (including the enclosed Transaction Set) error resulting in the rejection of the entire Functional Group.
   a. A v5010 999 must not be returned if there are errors not resulting in the rejection of the Functional Group and enclosed Transaction Set.
2. A v5010 277 must always be returned for an Interchange, Functional Group and Transaction Set that complies with X12 v5010 276 requirements.
   a. A v5010 277 may contain either the appropriate STC Claim or Line Level Status Information segment(s) in the case of a business level error or the data segments containing the requested claim status details.

5.3. Test Scripts Assumptions

1. All communications sessions and logons are valid; no error conditions are created or encountered.
2. Test scripts will test ONLY for valid and invalid X12 Interchange, Functional Group, Transaction Set and will not test for v5010 277 data content.
3. Test scripts will test the following error conditions:
    a. Invalid X12 Interchange (ISA control number match error)
    b. Invalid Functional Group (GS/GE control number match error)
    c. Invalid Transaction Set (missing required segment)
4. Test scripts will test the following valid conditions:
    a. Valid X12 Interchange Control Segments
    b. Valid Functional Group Control Segments
    c. Valid X12 Transaction Set
5. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

5.4. Detailed Step-By-Step Test Script

REMINDER: CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [4]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [5]
1.	A v5010 999 is returned on an invalid Functional Group (Key Rule Requirement #1)	An X12 Interchange containing only a v5010 999		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
2.	A v5010 999 is not returned on a valid X12 Interchange (Key Rule Requirement #1.a)	No v5010 999 returned		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
3.	A v5010 277 Claim Status Response transaction set is always returned for a valid v5010 276 Claim Status Inquiry Transaction set (Key Rule Requirement #2)	An X12 Interchange is returned containing only a v5010 277 transaction set		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

[4] A checkmark in the box indicates the stakeholder type to which the test applies.

[5] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

6. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Companion Guide Requirements Test Scenario

6.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

1. All Claim Status CORE-certified entities' Companion Guides covering the v5010 276/277 claim status inquiry and response transactions must follow the format/flow as defined in the CAQH CORE Master Companion Guide Template for HIPAA Transactions. (§4.7.1)
2. This rule does not require any Claim Status CORE-certified entity to modify any other existing companion guides that cover other HIPAA-adopted transaction implementation guides.

6.2. Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Companion Guide Requirements. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

Conformance with this rule is considered achieved by health plans (or information sources) if all of the following criteria are achieved:

Submission to a CAQH CORE-authorized Testing Vendor the following:

1. A copy of the table of contents of its official v5010 276/277 companion document.
2. A copy of a page of its official v5010 276/277 companion document depicting its conformance with the format for specifying the v5010 276/277 data content requirements.

Such submission may be in the form of a hard copy paper document, an electronic document, or a URL where the table of contents and an example of the v5010 276/277 content requirements of the companion document is located.

6.3. Test Scripts Assumptions

1. The detailed content of the v5010 276/277 companion document will not be submitted to the CAQH CORE-authorized Testing Vendor.
2. The detailed content of the v5010 276/277 companion document will not be examined nor evaluated.
3. Test script will test ONLY that the table of contents of the companion document is:
    a. Customized and specific to the entity undergoing this test
    b. Conforms to the flow as specified in the Table of Contents of the CAQH CORE Master Companion Document Template
    c. Conforms to the presentation format for depicting segments, data elements and codes as specified in the CAQH CORE v5010 276/277 Companion Document Template
4. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

6.4. Detailed Step-By-Step Test Script

REMINDER: CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [6]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [7]
1.	Companion Document conforms to the flow and format of the CAQH CORE Master Companion Document Template	Submission of the Table of Contents of the 276/277 companion document, including an example of the v5010 276/277 content requirements		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
2.	Companion Document conforms to the format for presenting each segment, data element and code flow and format of the CAQH CORE Master Companion Document Template	Submission of a page of the v5010 276/277 companion document depicting the presentation of segments, data elements and codes showing conformance to the required presentation format		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

[6] A checkmark in the box indicates the stakeholder type to which the test applies.

[7] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

7. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Batch Response Time Requirements Test Scenario

7.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Claim Status Batch Response Time Requirements

1. Maximum response time when processing in batch mode for the receipt of a v5010 277 response to a v5010 276 inquiry submitted by a provider or on a provider's behalf by a clearinghouse/switch by 9:00 pm Eastern time of a business day must be returned by 7:00 am Eastern time the following business day. A business day consists of the 24 hours commencing with 12:00 am (Midnight or 0000 hours) of each designated day through 11:59 pm (2359 hours) of that same designated day. The actual calendar day(s) constituting business days are defined by and at the discretion of each health plan or information source. (§4.5)
2. v5010 999 responses must be available to the submitter within one hour of receipt of the batch: to the provider in the case of a batch of v5010 276 inquiries and to the health plan (or information source) in the case of a batch of v5010 277 responses. (§4.5.1)
3. Conformance with this maximum response time rule shall be considered achieved if 90 percent of all required responses as specified in the Claim Status Batch Acknowledgements Requirements are returned within the specified maximum response time as measured within a calendar month. (§4.5.2)
4. Each CORE-certified entity must demonstrate its conformance with this maximum response time rule by demonstrating its ability to capture, log, audit, match and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners. (§4.5.2)

7.2. Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Batch Response Time Requirements. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

1. Capturing, logging, auditing, matching and reporting the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and its trading partners.

7.2.1. Test Scripts Assumptions

1. All transactions, data, communications session are valid; no error conditions are created or encountered.
2. The provider's PMS/HIS system generates all of the required data necessary for its clearinghouse to generate the batch V5010 X12 276 claim status inquiries.
3. The provider's clearinghouse's EDI management system generates a syntactically correct X12 interchange containing the v5010 276 claim status inquiry, therefore, no v5010 999 acknowledgement is to be returned by the health plan's system.
4. All HTTP/S communications sessions between all parties are successfully established with the respective Internet portals communications servers; therefore, no HTTP POST error messages are created by any of communications servers.
5. The health plan's system successfully locates and verifies the claim identified in the v5010 276 inquiry and outputs the required data required by its EDI management system to successfully generate a syntactically correct X12 interchange containing the v5010 277 response.
6. The health plan's EDI management system generates a syntactically correct X12 interchange containing the v5010 277 claim status response.
7. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

7.3. Detailed Step-By-Step Test Script:

REMINDER: CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [8]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [9]
1.	Verify that outer most communications module(s) transmits all required data elements in the claim status inquiry message. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #4)	Output a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☒	☐	☒	☒	☐

[8] A checkmark in the box indicates the stakeholder type to which the test applies.

[9] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [8]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [9]
2.	Verify that outer most communications module(s) captures, assigns, logs and links all required data elements from the V5010 X12 277 Interchange to the submitted V5010 X12 276 Interchange. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #4)	Output a system-generated audit log report showing all required data elements		□ Pass	□ Fail	☒	□	☒	☒	□
3.	Verify that outer most communications module(s) transmits all required data elements in the claim status response message. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #4)	Output a system-generated audit log report showing all required data elements		□ Pass	□ Fail	□	☒	☒	☒	□
4.	Verify that outer most communications module(s) captures, assigns, logs and links all required data elements from the X12/v5010 276 Interchange to the submitted V5010 X12/277 Interchange. If transactions use an alternate communication method to HTTP/S, entities must store enough	Output a system-generated audit log report showing all required data elements		□ Pass	□ Fail	□	☒	☒	☒	□

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [8]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [9]
	information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (**Key Rule Requirement #4**)									

8. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Real Time Response Time Requirements Test Scenario

8.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Real Time Mode Response Time Requirements

1. Maximum response time when processing in real time mode[10] for the receipt of a v5010 277 (or in the case of an error, a v5010 999 response from the time of submission of a v5010 276 inquiry must be 20 seconds (or less). v5010 999 response rejections must be returned within the same response timeframe. (§4.4)
2. Conformance with this maximum response time rule shall be considered achieved if 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month. (§4.4)
3. Each Claim Status CORE-certified entity must demonstrate its conformance with this maximum response time rule by demonstrating its ability to capture, log, audit, match and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and the corresponding data received from its trading partners. (§4.4.1)

8.2. Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status Real Time Response Time Requirements. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

1. Capturing, logging, auditing, matching and reporting the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and its trading partners.

[10] Real-time mode is defined in the CORE Glossary of Terms.

8.3. Test Scripts Assumptions

1. All transactions, data, communications session are valid; no error conditions are created or encountered.
2. The provider's PMS/HIS system generates a syntactically correct X12 interchange containing the v5010 276 claim status inquiry, therefore, no v5010 999 acknowledgement is to be returned by the health plan's system.
3. The provider's PMS/HIS system's communications module successfully establishes the HTTP/S communication session with the health plan's Internet portal communications server; therefore, no HTTP POST error message is created by the health plan's communications server.
4. The health plan's system successfully locates and verifies the claim identified in the v5010 276 inquiry and outputs the required data required by its EDI management system to successfully generate a syntactically correct X12 interchange containing the v5010 277 response.
5. The health plan's EDI management system generates a syntactically correct X12 interchange containing the v5010 277 claim status response.
6. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

8.4. Detailed Step-By-Step Test Script:

REMINDER: CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [11]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [12]
1.	Verify that outer most communications module(s) transmits all required data elements in the claim status inquiry message. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #3)	Output a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☒	☐	☒	☒	☐
2.	Verify that outer most communications module(s) captures, assigns, logs and links all required data elements from the V5010 X12/277 Interchange to the submitted V5010 X12/276 Interchange. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in	Output a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☒	☐	☒	☒	☐

[11] A checkmark in the box indicates the stakeholder type to which the test applies.

[12] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [11]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [12]
	addition to the times that the request was received and response was sent (Key Rule Requirement #3)									
3.	Verify that outer most communications module(s) transmits all required data elements in the claim status response message. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #3)	Output a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
4.	Verify that outer most communications module(s) captures, assigns, logs and links all required data elements from the V5010 X12/276 Interchange to the submitted V5010 X12/277 Interchange. If transactions use an alternate communication method to HTTP/S, entities must store enough information from the X12 transaction to uniquely identify the transmission in addition to the times that the request was received and response was sent (Key Rule Requirement #3)	Output a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

9. CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status System Availability Test Scenario

9.1. Key Rule Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

System Availability Requirements

1. System availability must be no less than 90 percent per calendar week for both real-time and batch processing modes. This will allow for health plan, (or other information source) clearinghouse/switch or other intermediary system updates to take place within a maximum of 24 hours per calendar week for regularly scheduled downtime. (§4.6.1)

Reporting Requirements

2. Scheduled Downtime

   Claim Status CORE-certified health plans (or information sources), clearinghouses/switches or other intermediaries must publish their regularly scheduled system downtime in an appropriate manner (e.g., on websites or in companion guides) such that the healthcare provider can determine the health plan's system availability so that staffing levels can be effectively managed. (§4.6.2.1)

3. Non-Routine Downtime

   For non-routine downtime (e.g., system upgrade), an information source must publish the schedule of non-routine downtime at least one week in advance. (§4.6.2.2)

4. Unscheduled Downtime

   For unscheduled/emergency downtime (e.g., system crash), an information source will be required to provide information within one hour of realizing downtime will be needed. (§4.6.2.3)

Other Requirements

5. No response is required during scheduled downtime(s). (§4.6.2.4)
6. Each health plan, (or other information source) clearinghouse/switch or other intermediary will establish its own holiday schedule and publish it in accordance with the rule above. (§4.6.2.5)

9.2. Conformance Testing Requirements

These scenarios test the following conformance requirements of CAQH CORE Claim Status (276/277) Infrastructure Rule: Claim Status System Availability. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, Claim Status CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario.

Demonstrate its ability to publish to its trading partner community the following schedules:

1. Its regularly scheduled downtime schedule, including holidays.
2. Its notice of non-routine downtime showing schedule of times down.
3. A notice of unscheduled/emergency downtime notice.

9.3. Test Scripts Assumptions

1. The entity has implemented in its production environments the necessary policies, procedures and method(s) required to conform to the requirements of Claim Status System Availability.
2. The Claim Status CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE Claim Status (276/277) Infrastructure Rule requirements of the rule.

9.4. Detailed Step-By-Step Test Script

REMINDER: CORE Certification Testing not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [13]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [14]
1.	Publication of regularly scheduled downtime, including holidays and method(s) for such publication (Key Rule Requirement #2)	Submission of actual published copies of regularly scheduled downtime including holidays and method(s) of publishing		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
2.	Publication of non-routine downtime notice and method(s) for such publication (Key Rule Requirement #3)	Submission of a sample notice of non-routine downtime including scheduled of down time and method(s) of publishing		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
3.	Publication of unscheduled/emergency downtime notice and method(s) for such publication (Key Rule Requirement #4)	Submission of a sample notice of unscheduled/emergency downtime including method(s) of publishing		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

[13] A checkmark in the box indicates the stakeholder type to which the test applies.

[14] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

10. CAQH CORE Connectivity Rule vC2.2.0 Test Scenario

10.1. Key Rule Requirements

<u>Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.</u>

Requires a CAQH CORE Connectivity Rule vC2.2.20 CORE-certified Health Plan and Health Plan Vendor to implement a Server and to:

1. Implement Server capability to support both Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.1, §4.2, §6.3.1)
2. Implement Server capability to support both Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.1, §4.2, §6.3.2)
3. Implement Server capability and enforce one of two specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.1)
4. Have a capacity plan such that it can receive and process a large number of single concurrent real-time transactions via an equivalent number of concurrent connections. (§4.3.5.1)
5. Have the capability to receive and process large batch transaction files if batch is supported. (§4.3.5.2)
6. Publish detailed specifications in a Connectivity Companion Guide on its public web site as required by the appropriate CAQH CORE Companion Guide Rule. (§4.3.7)

If a CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Health Plan and Health Plan Vendor elects to optionally implement a Client, it is required to:

7. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.1, §4.2, §6.3.1)
8. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.1, §4.2, §6.3.2)
9. Implement Client capability to support both specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.1)

10.1. Key Rule Requirements

Requires a CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Clearinghouse and other Intermediaries to implement a Server and to:

10. Implement Server capability to support both Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.2, §4.2, §6.3.1)
11. Implement Server capability to support both Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.2, §4.2, §6.3.2)
12. Implement Server capability and enforce one of two specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.2)
13. Have a capacity plan such that it can receive and process a large number of single concurrent real-time transactions via an equivalent number of concurrent connections. (§4.3.5.1)
14. Have the capability to receive and process large batch transaction files if batch is supported. (§4.3.5.2)
15. Publish detailed specifications in a Connectivity Companion Guide on its public web site as required by the appropriate CAQH CORE Companion Guide Rules. (§4.3.7)

Requires a CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Clearinghouse and other Intermediaries to implement a Client and to:

16. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.2, §4.2, §6.3.1)
17. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.2, §4.2, §6.3.2)
18. Implement Client capability to support both specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.2)

Requires a CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Provider and Provider Vendor to implement a Client and to:

19. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.3, §4.2, §6.3.1)
20. Implement Client capability to support one of two Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.3, §4.2, §6.3.2)
21. Implement Client capability to support both specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.3)

If a CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Provider and Provider Vendor elects to optionally implement a Server, it is required to:

22. Implement Server capability to support both Message Envelope Standards and Message Exchanges specified in the rule for Real Time. (§4.1.3, §4.2, §6.3.1)
23. Implement Server capability to support one of two Message Envelope Standards and Message Exchanges specified for Batch if Batch is offered. (§4.1.3, §4.2, §6.3.2)
24. Implement Server capability and enforce one of two both specified Submitter Authentication Standards for both Real Time and/or Batch. (§4.1.3)

10.1. Key Rule Requirements

Requires all CAQH CORE Connectivity Rule vC2.2.0 CORE-certified Message Receivers to:

25. Track the times of any received inbound messages. (§4.3.4.1)
26. Respond with the outbound message for the received inbound message. (§4.3.4.1)
27. Include the date and time the message was sent in HTTP+MIME or SOAP+WSDL Message Header tags. (§4.3.4.1)

Specifies:

28. Message Enveloping specifications for HTTP MIME Multipart (Envelope Standard A). (§4.2.1)
29. HTTP MIME Multipart payload attachment handling. (§4.2.1.8)
30. Message Enveloping specifications for SOAP+WSDL (Envelope Standard B). (§4.2.2)
31. XML Schema specification for SOAP. (§4.2.2.1)
32. Web Services Definition Language (WSDL) specification. (§4.2.2.2)
33. SOAP payload attachment handling. (§4.2.2.11)
34. Request and response handling for real time, batch, and batch response pickup. (§4.3.1)
35. Submitter authentication and authorization handling. (§4.3.2)
36. Error handling for both Envelope Messaging Standards. (§4.3.3)
37. Envelope metadata fields, including descriptions, intended use syntax and value-sets applicable to both Enveloping Messaging Standards. (§4.4)

10.2. Conformance Testing Requirements

The CORE Detailed Step-By-Step Test Scripts will not include comprehensive testing requirements for all possible permutations of the CAQH CORE Connectivity Rule vC2.2.0.

Conformance must be demonstrated by successful completion of the Detailed Step-By-Step Test Scripts specified below with a CAQH CORE-authorized Testing Vendor.

The Detailed Step-By-Step Test Scripts specify each specific test that must be completed by each stakeholder type for both Real Time and Batch communications. There are one or more Detailed Step-By-Step Test Scripts for each of the following conformance testing requirements of the CAQH CORE Connectivity Rule vC2.2.0. Batch Connectivity Test Scripts are only required to be completed if an entity supports Batch communications.

There may be other requirements of the rule not specified here or in The Detailed Step-By-Step Test Scripts. Notwithstanding, CAQH CORE Connectivity Rule vC2.2.0 CORE-certified entities are required to comply with all specifications of the rule not included in these Conformance Testing Requirements and Detailed Step-by-Step Test Scripts.

1. A health plan or health plan vendor must demonstrate it has implemented the server specifications for both Message Enveloping Standards.
2. A health plan or health plan vendor must demonstrate it has implemented one of the two submitter authentication standards.
3. A clearinghouse, switch or other intermediary must demonstrate it has implemented the server specifications for both Message Envelope Standards.
4. A clearinghouse, switch or other intermediary must demonstrate it has implemented the client specifications for one of the two Message Envelope Standards.
5. A clearinghouse that handles submissions to health plan must demonstrate it has implemented both submitter authentication standards.
6. A provider or provider vendor must demonstrate it has implemented the client specifications for one of the two Message Envelope Standards.
7. A provider or provider vendor must demonstrate it has implemented both submitter authentication standards.

10.3. Test Scripts Assumptions

1. All tests will be conducted over HTTP/S.
2. The message payload is an X12 Interchange.
3. No editing or validation of the message payload will be performed.
4. All submitter authentications are valid; no error conditions are created or encountered.
5. Testing will not be exhaustive for all possible levels of submitter authentication.
6. Test scripts will test for the ability to log, audit, track and report on the required data elements.
7. Rule specifications addressing payload attachment handling are not being tested.
8. Rule specifications addressing error handling are not being tested.
9. The test scripts will not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

10.4. Detailed Step-by-Step Test Script

REMINDER: CORE Certification is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. See Test Assumption above.

NOTE: The references in parentheses after each test script are references to the above rule items for which the test script is testing – items could be referring to Key Rule Requirement(s), the Conformance Testing Requirement(s) or the associated Test Script Assumption(s). An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	**Health Plan**	**Clearinghouse**	**Vendor**	**N/A** [16]
Real Time Connectivity Test Scripts										
1.	Implement and enforce **one of two** Submitter Authentication standards on communications **server** (Key Rule Requirement #3 and #12)									
1.1	Implement and enforce use of Username/Password over SSL on communications **server** (Key Rule Requirement #3 and #12)	Communications server accepts a valid logon by a client using Username/Password, which is embedded in the message envelope as specified in the CAQH CORE Connectivity Rule v2.2.0		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
1.2	Implement and enforce use of X.509 Certificate over SSL on communications **server** (Key Rule Requirement #3 and #12)	Communications server accepts a valid logon by a client using X.509 Certificate over SSL		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
2.	On the authenticated connection as per Test #1, implement capability to support **both** Message Envelope Standards and envelope metadata for Real Time as a communications **server** (Key Rule Requirement #1, #10 and #37)									
2.1	Implement SOAP+WSDL Message Envelope Standard and envelope metadata as a	Communications server accepts a valid logon by a client conforming to the		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

[15] The checkmark in each box below indicates the stakeholder type to which the test script applies.

[16] If you believe a specific test, or a portion of a specific test, does not apply to your system, check the N/A box and submit a statement describing your rationale.

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	**Health Plan**	**Clearinghouse**	**Vendor**	**N/A** [16]
	communications **server** (Key Rule Requirement #1, #10 and #37)	SOAP+WSDL envelope and metadata specifications, and successfully completes the Real-time message interactions as specified in §6.3.1 of the CAQH CORE Connectivity Rule v2.2.0								
2.2	Implement HTTP MIME Multipart Message Envelope Standard and envelope metadata as a communications **server** (Key Rule Requirement #1, #10 and #37)	Communications server accepts a valid logon by a client conforming to the HTTP MIME Multipart envelope and metadata specifications, and successfully completes the Real-time message interactions as specified in §6.3.1 of the CAQH CORE Connectivity Rule v2.2.0.		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
3.	Implement capability to support **both** Submitter Authentication standards as a communications **client** (Key Rule Requirement #18, #21)									
3.1	Implement Username/Password submitter authentication method as a communications **client** (Key Rule Requirement #18, #21, and #24)	Client successfully logs on to a communications server with Username/Password, which is embedded in the message envelope as specified in the CAQH CORE Connectivity Rule v2.2.0.		☐ Pass	☐ Fail	☒	☐	☒	☒	☐
3.2	Implement X.509 certificate submitter authentication method as a communications **client** (Key Rule Requirement #18, #21, #24)	Client successfully logs on to a communications server with X.509 certificate		☐ Pass	☐ Fail	☒	☐	☒	☒	☐
4.	On the authenticated connection as per Test #3, implement capability to support **one of two** Message Envelope Standards and envelope metadata for Real Time as a communications **client** (Key Rule Requirement #16, #19 and #37)									

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [16]
4.1	Implement SOAP+WSDL Message Envelope Standard and envelope metadata as a communications **client** (Key Rule Requirement #16, #19 and #37)	Communications client successfully logs on to a communications server using the SOAP+WSDL Message Envelope Standard and envelope metadata specifications, and successfully completes the Real-time message interactions as specified in §6.3.1 of the CAQH CORE Connectivity Rule v2.2.0.		□ Pass	□ Fail	☒	□	☒	☒	□
4.2	Implement HTTP MIME Multipart Message Envelope Standard and envelope metadata as a communications **client** (Key Rule Requirement #16, #19 and #37)	Communications client successfully logs on to a communications server using the HTTP MIME Multipart Message Envelope Standard and envelope metadata specifications, and successfully completes the Real-time message interactions as specified in §6.3.1 of the CAQH CORE Connectivity Rule v2.2.0.		□ Pass	□ Fail	☒	□	☒	☒	□
5.	Verify that communications **server** creates, assigns, logs, links the required metadata elements to message payload (Key Rule Requirement #25 and #27)	Output a system generated audit log report showing all required data elements		□ Pass	□ Fail	□	☒	☒	☒	□
6.	Verify that communications **client** creates, assigns, logs, links the required metadata elements to message payload (Key Rule Requirement #25 and #27)	Output a system generated audit log report showing all required data elements		□ Pass	□ Fail	☒	□	☒	☒	□
Batch Connectivity Test Scripts (Required only if Batch is supported)										

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [16]
7.	Implement and enforce **one of two** Submitter Authentication standards on communications **server** (Key Rule Requirement #3 and #12)									
7.1	Implement and enforce use of Username/Password over SSL on communications **server** (Key Rule Requirement #3 and #12)	Communications server accepts a valid logon by a client using Username/Password, which is embedded in the message envelope as specified in the CAQH CORE Connectivity Rule v2.2.0		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
7.2	Implement and enforce use of X.509 Certificate over SSL on communications **server** (Key Rule Requirement #3 and #12)	Communications server accepts a valid logon by a client using X.509 Certificate over SSL		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
8.	On the authenticated connection as per Test #7, implement capability to support **both** Message Envelope Standards and envelope metadata for Batch as a communications **server** (Key Rule Requirement #2, #11 and #37)									
8.1	Implement SOAP+WSDL Message Envelope Standard and envelope metadata as a communications **server** (Key Rule Requirement #2, #11 and #37)	Communications server accepts a valid logon by a client conforming to the SOAP+WSDL envelope and metadata specifications, and successfully completes the Batch message interactions as specified in §6.3.2 of the CAQH CORE Connectivity Rule v2.2.0.		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
8.2	Implement HTTP MIME Multipart Message Envelope Standard and envelope metadata as a communications **server** (Key Rule Requirement #2, #11 and #37)	Communications server accepts a valid logon by a client conforming to the HTTP MIME Multipart envelope and metadata specifications, and successfully completes the Batch message interactions as specified in §6.3.2 of the CAQH CORE Connectivity Rule v2.2.0.		☐ Pass	☐ Fail	☐	☒	☒	☒	☐

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [16]
9.	Implement capability to support **both** Submitter Authentication standards as a communications **client** (Key Rule Requirement #18, #21)									
9.1	Implement Username/Password submitter authentication method as a communications **client** (Key Rule Requirement #18, #21, and #24)	Client successfully logs on to a communications server with Username/Password, which is embedded in the message envelope as specified in the CAQH CORE Connectivity Rule v2.2.0		□ Pass	□ Fail	☒	□	☒	☒	□
9.2	Implement X.509 certificate submitter authentication method as a communications **client** (Key Rule Requirement #18, #21, #24)	Client successfully logs on to a communications server with X.509 certificate		□ Pass	□ Fail	☒	□	☒	☒	□
10.	On the authenticated connection as per Test #9, implement capability to support **one of two** Message Envelope Standards and envelope metadata for Batch as a communications **client** (Key Rule Requirement #16, #19 and #37)									
10.1	Implement SOAP+WSDL Message Envelope Standard and envelope metadata as a communications **client** (Key Rule Requirement #17, #20, and #37)	Communications client successfully logs on to a communications server using the SOAP+WSDL Message Envelope Standard and envelope metadata specifications, and successfully completes the Batch message interactions as specified in §6.3.2 of the CAQH CORE Connectivity Rule v2.2.0.		□ Pass	□ Fail	☒	□	☒	☒	□

Test #	Criteria	Expected Result	Actual Result	Pass/Fail		Stakeholder [15]				
						Provider	Health Plan	Clearinghouse	Vendor	N/A [16]
10.2	Implement HTTP MIME Multipart Message Envelope Standard and envelope metadata as a communications **client** (Key Rule Requirement #17, #20, and #37)	Communications client successfully logs on to a communications server using the HTTP MIME Multipart Message Envelope Standard and envelope metadata specifications, and successfully completes the Batch message interactions as specified in §6.3.2 of the CAQH CORE Connectivity Rule v2.2.0.		☐ Pass	☐ Fail	☒	☐	☒	☒	☐
11.	Verify that communications **server** creates, assigns, logs, links the required metadata elements to message payload (Key Rule Requirement #25 and #27)	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☒	☒	☐
12.	Verify that communications **client** creates, assigns, logs, links the required metadata elements to message payload (Key Rule Requirement #25 and #27)	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☒	☐	☒	☒	☐

11. CAQH CORE SOAP Connectivity Rule vC4.0.0 Test Scenario

11.1. CAQH CORE SOAP Connectivity Rule vC4.0.0 Key Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Transport, Security, Authentication and Authorization Requirements (§3.2)

- Use of HTTP Version 1.1 over the public Internet is required as a transport method.
- Transport Layer Security (TLS) Version 1.2 (or higher).
    a. This does not preclude the optional use of TLS 1.3 (or a higher version) for connectivity with trading partners whose security policies require the enhanced security afforded by TLS 1.3 or higher.
- SOAP Version 1.2 or higher
- WSDL Version 1.1 or higher
- X.509 Digital Certification addressing authentication is required.
- OAuth 2.0 or higher addressing authorization is required.

Processing Mode (§3.7.1)

- Required Processing Mode Table specifies the comprehensive and normative processing mode requirements (i.e., Real Time and/or Batch) for the transactions addressed by this rule (§4.4.3)

Payload Type Table (§3.7.2)

- Required Payload Type Table (§4.4.3) specifies the comprehensive and normative identifiers for the CORE Envelope Metadata Payload Type Element as defined in the Table of CORE Envelope Metadata. (§4.4.2.)
- Payload Type identifiers specified in Payload Type Table apply when an entity is exchanging transactions addressed by this rule in conformance with the requirements specified in §4 and subsections.

11.2. CAQH CORE SOAP Connectivity Rule vC4.0.0 Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE SOAP Connectivity Rule v4.0.0. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario. Note: Clearinghouses and/or vendors undergoing CORE certification testing should refer to Detailed Step-by-Step Test Scripts for applicable test scripts.

- A HIPAA covered health plan must demonstrate it has implemented the server specifications for SOAP version 1.2.
- A HIPAA covered health plan must demonstrate it has implemented the X.509 authentication requirement.
- A HIPAA covered health plan must demonstrate it has implemented the server specifications for OAuth 2.0
- A HIPAA covered provider must demonstrate it has implemented the client specifications for SOAP version 1.2.
- A HIPAA covered provider must demonstrate it has implemented the X.509 authentication requirement.

11.3. CAQH CORE SOAP Connectivity Rule vC4.0.0 Test Scripts Assumptions

- All tests will be conducted over HTTP/S.
- The message payload is an X12 Interchange.
- No editing or validation of the message payload will be performed.
- Authentication will be tested for successful authentication with a valid certificate, and unsuccessful authentication using an invalid or missing certificate.
- Testing will not be exhaustive for all possible levels of authentication.
- Authorization will be tested for successful authorization with a valid token, and unsuccessful authorization using an invalid or missing token.
- Testing will not be exhaustive for all possible levels of authorization.
- The ability to log, audit, track and report on the required data elements as required by the conformance requirements of the CAQH CORE Infrastructure Rules will be addressed in each rule's test scripts.
- The test scripts will not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

11.4. CAQH CORE SOAP Connectivity Rule vC4.0.0 Detailed Step-by-Step Test Scripts

CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

The Detailed Step-by-Step Test Scripts below specify the stakeholder type to which each test script applies. A stakeholder may indicate that a specific test script does not apply to it. In this case the stakeholder is required to provide a rationale for why a specific test script is not applicable and be prepared for a review of the rationale with CAQH CORE staff.

When establishing a Certification Test Profile with a CAQH CORE-authorized Testing Vendor a Vendor will be given the option to indicate if the product it is certifying is a Provider-facing product or a Health Plan-facing product. Therefore, the Detailed Step-by-Step Test Scripts applicable to a Provider apply to a Provider-facing product. Similarly, Detailed Step-by-Step Test Scripts applicable to a Health Plan apply to a Health Plan-facing product.

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	**Stakeholder** *A checkmark in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
1	Implement and enforce use of X.509 Certificate over TLS on communications server	Communications server accepts a valid logon by a client using X.509 Certificate		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
2	Implement and enforce use of OAuth 2.0 over TLS on communications server	Communications server accepts a valid logon by a client using OAuth 2.0		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
3	On the authenticated and authorized connection implement SOAP+WSDL Message Envelope Standard and envelope metadata as a communications server	Communications server accepts a valid logon by a client conforming to the SOAP+WSDL envelope and metadata specifications		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
4	On an authenticated and authorized connection implement the Batch message interaction including receipt of a Batch of transactions, generation of acknowledgements and results	Server successfully receives batch(es) of the transactions and corresponding acknowledgements and responses specified in the respective transaction-specific infrastructure rule being tested		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
5	Implement X.509 certificate authentication method as a communications client	Client successfully logs on to a communications server with X.509 certificate		☐ Pass	☐ Fail	☐	☒	☐	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *A checkmark in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
6	On the authenticated connection implement SOAP+WSDL Message Envelope Standard and envelope metadata as a communications client	Communications client successfully logs on to a communications server using the SOAP+WSDL Message Envelope Standard and envelope metadata specifications		□ Pass	□ Fail	□	☒	□	☒	☒
7	On an authenticated connection implement the Batch message interaction including submission of a Batch of transactions, pickup of acknowledgements and results and submission of acknowledgement for results	Client successfully completes the submission and retrieval (pick up) of batch(es) of the transactions specified in the respective transaction-specific infrastructure rule being tested		□ Pass	□ Fail	□	☒	□	☒	☒
8	Verify that communications server creates, assigns, logs, links the required metadata elements to message payload	Output a system generated audit log report showing all required data elements		□ Pass	□ Fail	□	□	☒	☒	☒
9	Verify that communications client creates, assigns, logs, links the required metadata elements to message payload	Output a system generated audit log report showing all required data elements		□ Pass	□ Fail	□	☒	□	☒	☒

12. CAQH CORE REST Connectivity Rule vC4.0.0 Test Scenario

12.1. CAQH CORE REST Connectivity Rule vC4.0.0 Key Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the rule document for the specific language of the rule which governs. Section numbers in parentheses following each key requirement refer to the specific rule section which applies.

Transport, Security, Authentication and Authorization Requirements (§3.2)

- Use of HTTP Version 1.1 over the public Internet is required as a transport method.
- Transport Layer Security (TLS) Version 1.2 (or higher).
  a. This does not preclude the optional use of TLS 1.3 (or a higher version) for connectivity with trading partners whose security policies require the enhanced security afforded by TLS 1.3 or higher.
- JavaScript Object Notation (JSON)
- X.509 Digital Certification addressing authentication is required.
- OAuth 2.0 or higher addressing authorization is required.

General Specifications Applicable to REST APIs *(§5.2)*

- HIPAA-covered entities and their agents must be able to implement HTTP/S Version 1.1 over the public Internet as a transport method. (§5.2.1)
- The rule supports both Synchronous Real-time and Asynchronous Batch Processing for the transport of REST exchanges. (§5.2.2 – §5.2.5)
- If there is an error in processing the message at the HTTP layer the rule requires the use of the appropriate HTTP error or status codes as applicable to the error/status situation. (§5.2.6)
- CAQH CORE recommended best practice is for each trading partner to audit all the REST metadata and payload for each transaction. (§5.2.7)
- Message receivers (servers) are required to track the times of any received inbound messages and respond with the outbound message for a Payload (§5.2.8)
- A HIPAA-covered entity and its agent must have a capacity plan such that it can receive and process a large number of single concurrent Synchronous Real Time transactions via an equivalent number of concurrent connections. (§5.2.9)
- Synchronous Real Time response time must conform to the transaction's corresponding CAQH CORE Infrastructure Rule requirements. (§5.2.10)
- HIPAA-covered entity and its agent's messaging system must have the capability to receive and process large Batch transaction files if the entity supports Asynchronous Batch transactions. (§5.2.11)

12.1. CAQH CORE REST Connectivity Rule vC4.0.0 Key Requirements

Specifications for REST API Uniform Resource Identifiers (URI) Paths *(§5.3)*

- The rule requires message receivers (servers) to communicate the version of the CAQH CORE Connectivity Rule implemented and version of the REST API through the URI Path. (§5.3.1)
- This rule requires the use of standard naming conventions for REST API endpoints to streamline and support uniform REST implementations as defined in Table 5.3.2. (§5.3.2)

REST HTTP Request Method Requirements *(§5.4)*

- The rule specifies the use of HTTP Methods POST and GET. However, entities may choose to use additional HTTP Methods (e.g., PUT, PATCH, DELETE, etc.). (§5.4)

REST HTTP Metadata, Descriptions, Intended Use and Values *(§5.5)*

- The rule specifies metadata that are required to be used for HTTP Requests and HTTP Responses for REST exchange as defined in Table 5.5. (§5.5)

12.2. CAQH CORE REST Connectivity Rule vC4.0.0 Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE REST Connectivity Rule v4.0.0. Other requirements of this rule that may not be listed below are not included in this test scenario. Notwithstanding, CORE-certified entities are required to comply with all specifications of the rule not included in this test scenario. Note: Clearinghouses and/or vendors undergoing CORE certification testing should refer to Detailed Step-by-Step Test Scripts for applicable test~~s~~ scripts.

- A HIPAA covered health plan must demonstrate it has implemented the server specifications for OAuth 2.0.
- A HIPAA covered health plan must demonstrate it has implemented the X.509 authentication requirement.
- A HIPAA covered provider must demonstrate it has implemented the client specifications for OAuth 2.0.
- A HIPAA covered provider must demonstrate it has implemented the X.509 authentication requirement.

12.3. CAQH CORE REST Connectivity Rule vC4.0.0 Test Scripts Assumptions

- All tests will be conducted over HTTP/S.
- The message payload is an X12 Interchange.
- No editing or validation of the message payload will be performed.
- Authentication will be tested for successful authentication with a valid certificate, and unsuccessful authentication using an invalid or missing certificate.
- Testing will not be exhaustive for all possible levels of authentication.
- Authorization will be tested for successful authorization with a valid token, and unsuccessful authorization using an invalid or missing token.
- Testing will not be exhaustive for all possible levels of authorization.
- The ability to log, audit, track and report on the required data elements as required by the conformance requirements of the CAQH CORE Infrastructure Rules will be addressed in each rule's test scripts.
- The CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

12.4. CAQH CORE REST Connectivity Rule vC4.0.0 Detailed Step-by-Step Test Scripts

CORE Certification Testing is not exhaustive. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements that test for all possible permutations of each rule. An individual test script may be testing for more than one item, and, as noted in the "Stakeholder" column, each test script tests for the role of the Stakeholder(s) to which the test script applies.

The Detailed Step-by-Step Test Scripts below specify the stakeholder type to which each test script applies. A stakeholder may indicate that a specific test script does not apply to it. In this case the stakeholder is required to provide a rationale for why a specific test script is not applicable and be prepared for a review of the rationale with CAQH CORE staff.

When establishing a CORE Certification Test Profile with a CAQH CORE-authorized Testing Vendor a Vendor will be given the option to indicate if the product it is certifying is a Provider-facing product or a Health Plan-facing product. Therefore, the Detailed Step-by-Step Test Scripts applicable to a Provider apply to a Provider-facing product. Similarly, Detailed Step-by-Step Test Scripts applicable to a Health Plan apply to a Health Plan-facing product.

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *A checkmark in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
1	Implement and enforce use of X.509 Certificate over TLS on communications server	Communications server accepts a valid logon by a client using X.509 Certificate		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
2	Implement and enforce use of OAuth 2.0 Token over TLS on communications server	Communications server accepts a valid logon by a client using OAuth 2.0 Token		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
3	On the authenticated and authorized connection implement REST Message and Envelope metadata as a communications server over a valid REST API Uniform Resource Identifiers (URI)	Communications server accepts a valid logon by a client conforming to the REST envelope and metadata specifications		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
4	On an authenticated and authorized connection implement the REST synchronous message interaction including receipt of a Batch of transactions, generation of acknowledgements and results valid REST API Uniform Resource Identifiers (URI)	Server successfully receives batch(es) of the transactions and corresponding acknowledgements and responses specified in the respective transaction-specific infrastructure rule being tested		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	**Stakeholder** *A checkmark in the box indicates the stakeholder type to which the test applies*			
							Provider	**Health Plan**	**Clearinghouse**	**Vendor**
5	Implement X.509 certificate submitter authentication method as a communications client	Client successfully logs on to a communications server with X.509 certificate		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
6	On the authenticated connection implement OAuth as a communications client	Communications client successfully logs on to a communications server using OAuth		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
7	On an authenticated and authorized connection implement the REST synchronous message interaction including submission of a Batch of transactions, pickup of acknowledgements and results and submission of acknowledgement for results	Client successfully completes the submission and retrieval (pick up) of batch(es) of the transactions specified in the respective transaction-specific infrastructure rule being tested		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
8	Verify that communications server creates, assigns, logs, links the required metadata elements to message payload	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
9	Verify that communications client creates, assigns, logs, links the required metadata elements to message payload	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☐	☒	☒