Premium Payment CAQH CORE Certification Test Suite
Version PP.2.0
April 2022

Revision History For Premium Payment CAQH CORE Certification Test Suite

Version	Revision	Description	Date
3.0.0	Major	Phase IV CAQH CORE Voluntary Certification Test Suite balloted and approved by the CAQH CORE Voting Process.	September 2015
PP.1.0	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
PP.2.0	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

This CAQH CORE Certification Test Suite contains the requirements that must be met by an entity seeking CORE Certification on the CAQH CORE Premium Payment Operating Rules to be awarded a CORE® Certified Seal. As such, this Test Suite includes:

- Guidance as to the types of stakeholders to which the CAQH CORE Premium Payment Operating Rules apply and how to determine when a specific rule's detailed test script applies to a stakeholder

- For each Premium Payment CAQH CORE Operating Rule:
  - High level summary of key rule requirements
  - The specific conformance testing requirements
  - Test script assumptions
  - Detailed Step-By-Step Test Scripts

1.1. CORE Certification Guiding Principles

The CAQH CORE Guiding Principles apply to the entire set of operating rules, including the CAQH CORE Certification Test Suite. CORE Certification Testing is not exhaustive and does not use production-level testing. The CAQH CORE Certification Test Suite does not include comprehensive testing requirements to test for all possible permutations of each rule's requirements.

Entities seeking CORE Certification are required to adopt all rules of a set that apply to their business and will be responsible for all their own company-related testing resources, e.g., certain entities only support the enrollment and premium payment transactions and would only adopt rules pertaining to those transactions. CORE Certification will be available for both Real Time and Batch Processing Modes. In the CAQH CORE Premium Payment (820) Infrastructure Rule, Batch Processing Mode is required for premium payment transactions with Real Time Processing Mode optional.

CORE Certification Testing is required of any entity seeking CORE Certification.

The CORE Certification process has four components:[1]

1. Pre-certification Planning and Systems Evaluation
2. Signing and Submitting the CORE Pledge
3. CORE Certification Testing
4. Applying for the CORE Seal

After signing the CORE Pledge, an entity has 180 days to complete CORE Certification Testing and submit its application for CORE Certification. The CAQH CORE testing protocol is scoped only to demonstrate conformance with CAQH CORE Operating Rules, and not overall compliance with HIPAA; each entity applying for CORE Certification will sign a statement affirming that it is HIPAA-compliant to the best of its knowledge. (Signature is from executive-level management.) CORE Certification Testing is not exhaustive, (e.g., does not include production data, volume capacity testing, all specific requirements of each rule, or end-to-end trading partner testing). CAQH CORE will not oversee trading partner relationships; CORE-certified entities may work with non-CORE-certified entities if they so desire. The CORE Certification Testing Policy will be used to gain CORE Certification only; it does not outline trading partner implementation interoperability testing activities.

[1] https://www.caqh.org/core/core-certification-process

1.2. Eligibility for CORE Certification

CAQH CORE certifies all entities that create, transmit or use applicable administrative transactions. CAQH CORE also certifies products or services that facilitate the creation, transmission or use of applicable administrative transactions. CORE Certification Testing varies based on stakeholder type; entities successfully achieving CORE Certification will receive the CORE "Seal" that corresponds with their stakeholder type.

Associations, medical societies and the like are not eligible to become CORE-certified; instead, these entities will receive a CAQH CORE "Endorser" Seal after signing the Pledge. Endorsers are expected to participate in CAQH CORE public relations campaigns, provide CAQH CORE feedback and input when requested to do so, and encourage their members to consider participating in CAQH CORE.

1.3. Role of CAQH CORE-authorized Testing Vendors

To obtain a CORE Certification Seal, entities must successfully complete stakeholder-specific Detailed Step-by-Step Test Scripts in the CAQH CORE Certification Test Suite. Successful completion is demonstrated through proper documentation from a CAQH CORE-authorized Testing Vendor.

CAQH CORE-authorized Testing Vendors are companies that have expertise in healthcare transaction testing. They are chosen by CAQH CORE to conduct CORE Certification Testing for all published CAQH CORE Operating Rules using the CAQH CORE Certification Test Suite specific to each CAQH CORE Operating Rule set after undergoing a rigorous selection process by CAQH CORE. Alpha and Beta testing of their CORE Certification Testing Platform is performed by CAQH CORE Participants to ensure it aligns with the CAQH CORE Certification Test Suites.

NOTE: CORE Certification and CORE Certification Testing are separate activities. CORE Certification Testing is performed by entities seeking CORE Certification and supported by CAQH CORE-authorized Testing Vendors. CORE Certification is awarded by CAQH CORE after a review of the completed certification testing with a CAQH CORE-authorized Testing Vendor.

1.4. Applicability of this Document

All entities seeking CORE Certification must successfully complete CAQH CORE Certification Testing from a CAQH CORE-authorized Testing Vendor in accordance with the Premium Payment CAQH CORE Certification Test Suite. This is required to maintain standard and consistent test results and Premium Payment CAQH CORE rule conformance. There are no exceptions to this requirement.

While the CAQH CORE Premium Payment Operating Rules apply specifically to HIPAA-covered Health Plans, HIPAA-covered Providers, or their respective agents[2] (see §2.2.5), CORE Certification Seals are awarded to a broader range of entities including clearinghouses and vendors and are not limited only to HIPAA-covered entities. In general, all entities that create, transmit or use applicable administrative transactions may seek CORE Certification. CAQH CORE also certifies products or services that facilitate the creation, transmission or use of applicable administrative transactions.

Entities that can obtain CORE Certification Seals are categorized into four CORE Certification stakeholder types: Providers, Health Plans, Clearinghouses, and Vendors. While three of the four CORE Certification stakeholder types share names with HIPAA-covered entities – Health Plans, Providers, and Clearinghouse – for purposes of CORE Certification, these three CORE Certification stakeholder types encompass a broader group of entities than what is included in their respective HIPAA-covered definitions. For instance, the CORE Certification stakeholder type "Health Plan" also includes Third Party Administrators (TPAs) which generally are not defined as HIPAA-covered entities. Other examples of entities that fall into these CORE Certification stakeholder types are described in Section 2.2.5. Throughout the remainder of this document, unless otherwise specified, references to Provider, Health Plan, Clearinghouse, and Vendor are references to the CORE Certification stakeholder type categorizations.

[2] One who agrees and is authorized to act on behalf of another, a principal, to legally bind an individual in particular business transactions with third parties pursuant to an agency relationship. Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group, Inc. All rights reserved.

2. Guidance for Using This CAQH CORE Certification Test Suite

2.1. Structure of Test Scenarios for all Rules

Each test scenario for each rule contains the following sections:

- Key Rule Requirements
  - The CAQH CORE Premium Payment Operating Rule documents contains the actual rule language and are the final authority for all operating rule requirements
- Certification conformance testing requirements by rule
- Test assumptions by rule
- Detailed Step-By-Step Test Scripts addressing each conformance testing requirement by rule for each stakeholder type to which the test script applies

2.2. Determining CAQH CORE Stakeholder Type for CORE Certification

Each test script listed in the Detailed Step-by-Step Test Script Section for each Test Scenario is applicable to one or more of the stakeholder types specified in the Stakeholder columns. An entity may indicate that a specific test script does not apply to it. In this case the entity 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.

The CORE Certification stakeholder types to which the Detailed Step-by-Step Test Scripts apply are Provider, Health Plan, Clearinghouse, and Vendor.

2.2.1. CORE Certification Provider Stakeholder Type

The CORE Certification stakeholder type "Provider" includes, but is not limited to, a HIPAA-covered provider. The CORE Certification stakeholder type "Provider" may also include any entity, (i.e., an agent) that offers administrative services for a provider or group of providers, and may include other agents that take the role of provider in HIPAA-mandated standard transactions. Notwithstanding, HIPAA-covered Providers such as physicians, hospitals, dentists, and other providers of medical or health services are included in the CORE Certification stakeholder type. (See §2.2.5 for more detail.)

2.2.2. CORE Certification Health Plan Stakeholder Type

As noted above, the CORE Certification stakeholder type "Health Plan" includes, but is not limited to, HIPAA-covered health plans. The CORE Certification stakeholder type "Health Plan" is more akin to entities that the industry refers to as "payers," and includes Third Party Administrators (TPAs), contractors with Administrative Services Only (ASO) arrangements, and other agents that may conduct some or all elements of the HIPAA transactions on the behalf of a HIPAA-covered health plan. Notwithstanding, HIPAA-covered health plans such as self-insured health plans, health plan issuers, government health plans, and others are included in the CORE Certification stakeholder type. (See §2.2.5 for more detail.)

2.2.3. CORE Certification Clearinghouse Stakeholder Type

The CORE Certification stakeholder type "Clearinghouse" includes, but is not limited to, HIPAA-covered Health Care Clearinghouses. HIPAA defines a Health Care Clearinghouse as an entity that processes health information received in a non-standard format into a standard format, or vice versa[3]. For purposes of voluntary CORE Certification, any intermediary between a Provider and a Health Plan CORE Certification stakeholder type that performs some or all aspects of a HIPAA-mandated function or a Premium Payment CAQH CORE Operating Rule could be considered a CORE Certification Clearinghouse stakeholder type.

A company offering a broad array of employee benefits administration services may also perform a variety of activities to facilitate and enable the collection and exchange of information related to employee benefits, such as medical/health insurance, pensions, etc., could be considered a CORE Certification Clearinghouse stakeholder type. An insurance broker may also be viewed as a CORE Certification Clearinghouse stakeholder. Broadly defined, a broker is one who represents

[3] See 45 CFR 160.103

an insured in the solicitation, negotiation or procurement of contracts of insurance, and who may render services incidental to those functions. A broker may also be an agent of the insurer for certain purposes such as delivery of the policy or collection of the premium.

2.2.4. CORE Certification Vendor Stakeholder Type

An entity (hereafter vendor) may offer commercially available software products or services that enables a provider, a health plan or a clearinghouse to carry out HIPAA-required functions (e.g., standard transactions or a CAQH CORE Operating Rule). Such vendor's products or services also are eligible for CORE Certification. Vendors may also include companies offering commercially available software products or services to an employer or an employee benefits administration company, enabling it to automate the administration of the typical human resource functions performed by employee benefits administrators. Employee benefits typically include medical insurance, pension plans, individual retirement accounts (IRAs), vacation time, sick time, and maternity leave. In the context of this Premium Payment CAQH CORE Certification Test Suite, a vendor with commercially available products can seek CORE Certification for those products/services and must certify each of its specific products/services and product/service versions separately. (See §2.2.5 for more detail.)

2.2.5. Table of CORE Certification Stakeholder Types Examples

This table includes examples of entities that can obtain CORE Certified Seals. This table is not intended to be comprehensive and exhaustive and may not include all possible entities.

Examples of Entities that are included in the four CORE Certification Stakeholder Types[4]			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
HIPAA-covered Provider • Any person or organization who furnishes, bills, or is paid for medical or health services in the normal course of business[5] **Provider Agent** • Any entity that performs HIPAA-required functions or services for a provider or group of providers and may include other entities that take the role of provider in HIPAA-mandated standard transactions **Accountable Care Organizations** • Groups of doctors, hospitals, and other health care providers, who come together voluntarily to give	**HIPAA-covered Health Plan** Includes the following, singly or in combination:[6] • A group health plan • A health insurance issuer • An HMO • Part A or Part B of the Medicare program under title XVIII of the Act • The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq • An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)) • An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy	**HIPAA-covered Clearinghouse** A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: [7] • Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction • Receives a standard transaction from another entity and processes or	**Health Plan Vendor (Product)** • A vendor of commercially available software solutions for adjudication, claim processing, claim data warehousing, etc., for a health plan or its business associate *Note: A software solution vendor does not hold nor process data on behalf of its customer. This type of vendor is not a business associate of the health plan as defined under HIPAA.* **Health Plan Vendor (Services)** • An entity that holds and processes data on behalf of its health plan customer

4 For more information regarding stakeholder types contact CAQH CORE (CORE@CAQH.org)

5 Social Security Act, Section 1861 definitions for (u) and (s) are available online at https://www.ssa.gov/OP_Home/ssact/title18/1861.htm

6 U.S. 45 CFR 160.103

7 Ibid.

Examples of Entities that are included in the four CORE Certification Stakeholder Types[4]			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
coordinated high quality care to their Medicare patients[8] • A network of doctors, hospital, specialists, post-acute providers and even private companies like Walgreens that shares financial and medical responsibility for providing coordinated care to patients in hopes of limiting unnecessary spending[9] • A healthcare organization characterized by a payment and care delivery model that seeks to tie provider reimbursements to quality metrics and reductions in the total cost of care for an assigned population of patients • A health insurance issuer-formed ACO[10]	• An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers • The health care program for active military personnel under title 10 of the United States Code • The veterans' health care program under 38 U.S.C. chapter 17 • The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)) • The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq • The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq • An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq • The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28 • A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals. Any other individual or group plan, or combination of	facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity **Clearinghouse** • Brokers or mediates connectivity between a provider and a health plan either directly or through another clearinghouse • Receives administrative transactions from either a provider or a health plan and forwards to the intended recipient • Provides other services based on each entity's business model *Note: A clearinghouse is distinct from a Health Care Clearinghouse as defined under HIPAA in that it does NOT transform non-standard data/format into/out of the standard; rather it receives the standard data/format from another entity, a clearinghouse may disaggregate and re-aggregate transactions and then route/forward the transaction to another entity.* **Health Information Exchange (Health Information Service Provider)** • Provides secure transmission of clinical information between providers	• An entity to which a health plan has outsourced a business function(s) *Note: This type of vendor holds and processes data on behalf of a health plan e.g., eligibility/membership data; utilization management, health care services review request/response (referral/authorizations.) This type of vendor is defined as a business associate under HIPAA.* **Provider Vendor (Product)** • A vendor of commercially available software solutions for practice management, patient accounting, etc., to a health care provider or its business associate *Note: A software solution vendor does not hold nor process data on behalf of its customer. This type of vendor is not a business associate of the health plan as defined under HIPAA.* **Provider Vendor (Services)** • A billing/collection or financial services company to which a provider outsources some or all of its financial functions *Note: This type of vendor holds and processes data on behalf of a health care provider, e.g., eligibility verification, billing and collections. This type of vendor is defined as a business associate under HIPAA.*

8 https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html?redirect=/aco and http://innovation.cms.gov/initiatives/aco/

9 http://kaiserhealthnews.org/news/aco-accountable-care-organization-faq/

10 Ibid.

Examples of Entities that are included in the four CORE Certification Stakeholder Types[4]			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
	individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)) **Third Party Administrator (TPA)** • An organization that processes insurance claims or certain aspects of employee benefit plans for a separate entity. This can be viewed as "outsourcing" the administration of the claims processing, since the TPA is performing a task traditionally handled by the company providing the insurance or the company itself. Often, in the case of insurance claims, a TPA handles the claims processing for an employer that self-insures its employees.[11] • An insurance company may also use a TPA to manage its claims processing, provider networks, utilization review, or membership functions. While some third-party administrators may operate as units of insurance companies, they are often independent.[12] **Administrative Services Only (ASO)** • A contract under which a third party administrator or an insurer agrees to provide administrative services to an employer in exchange for a fixed fee per employee [13]	• Provides secure transaction of administration information between providers and health plans • Provides a "community of trust" for authentication of organizations and end users within an organization • May manage PKI digital certifications for the "community" • May transform messages to the form acceptable by the receiver • Forwards clinical information to another HIE for intercommunity information exchange **Employee Benefit Administrators** • Provides services to employers to administer and manage a variety of employee benefits, such as medical insurance, pensions, vacations, etc. **Health Insurance Marketplaces or Exchanges** [14] • Private exchanges which may predate the Affordable Care Act to facilitate insurance plans for employees of small and medium size businesses • Exchanges are not themselves insurers, so they do not bear risk themselves, but they do determine the insurance companies that are allowed to participate • Health Insurance Exchanges use electronic data interchange to transmit required information between the Exchanges and Carriers (trading	**Human Resource Software Vendor (Product or Service)** • A company that offers to employers or employee benefit administrators commercially available software or cloud-based services

11 https://en.wikipedia.org/wiki/Third-party_administrator

12 Ibid.

13 http://en.termwiki.com/EN/administrative_services_only_(ASO)_contract

14 https://en.wikipedia.org/wiki/Health_insurance_marketplace

Examples of Entities that are included in the four CORE Certification Stakeholder Types[4]			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
	• An arrangement in which an organization funds its own employee benefit plan such as a pension plan or health insurance program but hires an outside firm to perform specific administrative services, e.g., an organization may hire an insurance company to evaluate and process claims under its employee health plan while maintaining the responsibility to pay the claims itself [15] • An arrangement under which an insurance carrier, its subsidiary or an independent organization will handle the administration of claims, benefits, reporting and other administrative functions for a self-insured plan **Health Plan Agent** • Any entity that performs HIPAA-required functions or services for a health plan and may include other entities that take the role of a health plan in HIPAA-mandated standard transactions	partners), in particular enrollment information and premium payment information **Value Added Network**[16] • A Value-added Network (VAN) is a hosted service offering that acts as an intermediary between business partners sharing standards based or proprietary data via shared Business Processes.	

2.3. User Quick Start Guide

An entity can access a User Quick Start Guide specific to a set of CAQH CORE Operating Rules for which it is seeking certification when it initially establishes its testing profile on the CORE-authorized Testing Vendor's test site. The User Quick Start Guide is to be used in connection with CORE-authorized Testing Vendor's certification testing system. It is meant to serve as an instruction document for the design and general utility of the testing system and is not a step-by-step CORE Certification guide.

2.4. Guidance for Providers and Health Plans Seeking CAQH CORE Certification that work with Agents

Any Provider or Health Plan seeking CORE Certification must undergo certification testing in accordance with the CAQH CORE Certification Test Suite. However, a Provider or a Health Plan may also be CORE Certified when it outsources various functions to a third party, i.e., a Business Associate (referenced as an agent in the CAQH CORE Premium Payment Operating Rules). Thus, the Detailed Step-by-Step Test Scripts recognize that a Provider or a Health Plan may use a

15 http://www.investopedia.com/terms/a/administrative-services-only.asp

16 https://en.wikipedia.org/wiki/Value-added_network

Business Associate to perform some or all of the HIPAA-mandated functions required by the HIPAA-mandated standards and/or the HIPAA-mandated CAQH CORE Operating Rules on its behalf.

When a Provider or a Health Plan outsources some functions to a Business Associate, both the Provider or Health Plan and its respective Business Associate to which the functions are outsourced will need to undergo voluntary CORE Certification Testing in order for the Provider or the Health Plan to become CORE-certified. The requirements for meeting the CORE rule requirements for either a Provider or a Health Plan differ by situation and such variability is dependent on how the Provider or the Health Plan interacts with its Business Associate and what services (i.e., functions and capabilities) its Business Associate provides to it. For example, a Health Plan seeking Premium Payment CORE Certification that uses a clearinghouse may have some unique circumstances when undergoing certification testing. Because there is a clearinghouse between the Health Plan's system and the Provider's system, the clearinghouse will act as a "proxy" for some of the CORE Certification requirements outlined in the Premium Payment CAQH CORE Certification Test Suite.

Keep in mind that certification testing will differ by each Test Scenario and each Detailed Step-by-Step Test Script. Dependent upon the agreement between the Provider or the Health Plan and the clearinghouse, the Provider or the Health Plan may not have to undergo certification testing for some aspects of the rules. In such a case, the Provider or the Health Plan must provide a rationale statement which explains the situation to the CORE-authorized Testing Vendor for each test script for which the N/A option is chosen and the Provider or the Health Plan will need to be prepared for a review of the rationale with CAQH CORE staff.

3. CAQH CORE Premium Payment (820) Infrastructure Rule Test Scenario

3.1. CAQH CORE Premium Payment (820) Infrastructure Rule 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.

Processing Mode Requirements (§4.1)

- A HIPAA covered health plan or its agent must implement server requirements for Batch Processing Mode.
- A HIPAA covered health plan or its agent may optionally implement server requirements for Real Time Processing Mode.

Connectivity Requirements (§4.2)

- HIPAA-covered entity and its agent must be able to support the most recent published and CAQH CORE adopted version of the CAQH CORE Connectivity Rule.

System Availability Requirements (§4.3)

- A HIPAA-covered health plan or its agent's system availability must be no less than 90 percent per calendar week.
- A HIPAA-covered health plan and its agent may choose to use an additional 24 hours of scheduled system downtime per calendar quarter.
-
- A HIPAA covered health plan or its agent must publish their regularly scheduled system downtime in an appropriate manner.
- A HIPAA covered health plan or its agent must publish the schedule of non-routine downtime at least one week in advance.
- A HIPAA covered health plan or its agent must provide information within one hour of realizing downtime will be needed in the event of unscheduled/emergency downtime.
- No response is required during scheduled or unscheduled/emergency downtime(s).
- A HIPAA covered health plan or its agent must establish and publish its own holiday schedule.

Response Time Requirements (§4.4. §4.5)

- When an ASC X12N v5010 820 has been submitted in Real Time Processing Mode by any entity, an ASC X12C v5010 999 must be returned with 20 seconds.
- When an ASC X12N v5010 820 has been submitted in Batch Processing Mode by any entity by 9:00 pm Eastern Time of a business day, an ASC X12C v5010 999 must be available for pick up by 7:00 am Eastern Time on the third business day following submission.
- Each HIPAA covered entity must support this maximum response time to ensure that at least 90 percent of all required responses are returned within the specified maximum response time as measured within a calendar month.
- Each HIPAA covered entity must 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.

3.1. CAQH CORE Premium Payment (820) Infrastructure Rule Key Requirements

Use of Acknowledgements Requirements (§4.5, §4.7)

- When an ASC X12N v5010 820 has been submitted in Real Time Processing Mode by any entity, an ASC X12C v5010 999 must be returned to indicate acceptance, acceptance with errors, or rejection of the Functional Group of an ASC X12N v5010 820.
- When an ASC X12N v5010 820 has been submitted in Batch Processing Mode by any entity, an ASC X12C v5010 999 must be returned to indicate the acceptance, acceptance with errors, or rejection of the Functional Group of an ASC X12N v5010 820.
- The ASC X12C v5010 999 must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999.

Elapsed Time for Enrollment System Processing of Received Enrollment Data (§4.8)

- A HIPAA covered health plan must process the enrollment data in its internal enrollment application system within five business days following successful receipt and verification of the data.

Companion Guide Requirements (§4.9)

- A Companion Guide covering the ASC X12N v5010 820 published by a HIPAA covered health plan or its agent must follow the format/flow as defined in the CAQH CORE Master Companion Guide Template.

3.2. CAQH CORE Premium Payment (820) Infrastructure Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the ASC X12N v5010 820 Requirements. 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.

System Availability

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

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

Acknowledgements

- An ASC X12C v5010 999 is returned to indicate either acceptance, acceptance with errors, or rejection a Functional Group of an ASC X12N v5010 820.

Response Time

- Demonstrate the ability to capture, log, audit, match, and report the date (YYYYMMDD), time (HHMMSS) and control numbers from its own internal systems and its trading partners

3.2. CAQH CORE Premium Payment (820) Infrastructure Rule Conformance Testing Requirements

Companion Guide

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

- A copy of the table of contents of its official ASC X12N v5010 820 companion guide.
- A copy of a page of its official ASC X12N v5010 820 companion guide depicting its conformance with the format for specifying the ASC X12N v5010 820 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 companion guide is located.

3.3. CAQH CORE Premium Payment (820) Infrastructure Rule Test Scripts Assumptions

- The entity has implemented in its production environments the necessary policies, procedures and method(s) required to conform to the requirements of the System Availability requirements.
- The test scripts will not include comprehensive testing requirements to test for all possible permutations of the CAQH CORE requirements of the rule.
- All communications sessions and logons are valid; no error conditions are created or encountered.
- The health plan's EDI management system generates a syntactically correct ASC X12 interchange containing the ASC X12N v5010 820 and ASC X12C v5010 999 transactions.
- Test scripts will test ONLY for valid and invalid ASC X12 Interchange, Functional Group, Transaction Set control segments and will not test for ASC X12N v5010 820 and ASC X12C v5010 999 data content.
- The detailed content of the companion guide will not be submitted to the CAQH CORE-authorized Testing Vendor.
- The detailed content of the companion guide will not be examined nor evaluated.

3.4. CAQH CORE Premium Payment (820) Infrastructure Rule 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.

System Availability										
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	Publication of regularly scheduled downtime, including holidays and method(s) for such publication	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	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	Submission of a sample notice of unscheduled/emergency downtime including method(s) of publishing		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Acknowledgements										
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**
4	An ASC X12C v5010 999 is returned on a rejected ASC X12 Functional Group of ASC X12N v5010 820 in either real time or batch	An ASC X12C v5010 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
5	An ASC X12C v5010 999 is returned on any accepted ASC X12 Functional Group of an ASC X12N v5010 820 in either real time or batch	An ASC X12C v5010 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Response Time										
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	Verify that outer most communications module(s) transmits all required data elements in the message. If the entity uses an alternate communication method to HTTP/S, the entity must store enough information from the ASC X12 Interchange, Functional Group and Transaction Set to uniquely identify the transmission in addition to the times that the request was received and response was sent	Submission of the output of a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Companion Guide										
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**
7	Companion Guide conforms to the flow and format of the CAQH CORE Master Companion Guide Template	Submission of the Table of Contents of the 820 companion guide, including an example of the ASC X12N v5010 820 content requirements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
8	Companion Guide conforms to the format for presenting each segment, data element and code flow and format of the CAQH CORE Master Companion Guide Template	Submission of a page of the ASC X12N v5010 820 companion guide depicting the presentation of segments, data elements and codes showing conformance to the required presentation format		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

4. CAQH CORE Connectivity Rule vC3.1.0 Test Scenario

4.1. CAQH CORE Connectivity Rule vC3.1.0 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 and Submitter Authentication Requirements (§3.2, §4)

- Use of HTTP Version 1.1 over the public Internet is required as a transport method.
- Secure Sockets Layer (SSL) Version 3.0 is required for transport security.
- Transport Layer Security (TLS) Version 1.1 (or higher) may be implemented in lieu of SSL Version 3.0.

Processing Mode and PayloadType Identifier Requirements (§3.7)

- Processing Modes specified in the CORE-required Processing Mode and Payload Type Tables document must be supported.
    - Batch Processing Mode is required for
        - Institutional, professional and dental claims transactions, and
        - Health plan premium payment transactions, and
        - Benefit enrollment and maintenance transactions.
    - Both Real Time and Batch Processing Mode may be used for prior authorization transactions.
        - Either Real Time or Batch Processing Mode must be implemented.
- Payload Types specified in the CORE-required Processing Mode and Payload Type Tables document must be supported.

Transport, Message Envelope, Submitter Authentication, Message Envelope Metadata Requirements (§4 through §4.4.3.3)

- SOAP version 1.2 (as specified in **§**3.2).
- WSDL Version 1.1 (as specified in **§**3.2).
- SOAP Message Payload must be sent as an MTOM encapsulated object (**§**4.1.4, and specified in the 4.0.0 XSD schema).
- The X.509 digital certificate is the only submitter authentication method permitted (**§**4.1.2).
- The CORE Envelope Metadata is normative and must not be modified (**§** 4.1.3).
- Servers must publish detailed specifications in a Connectivity Companion Document on the entity's public web site (**§**4.3).

4.2. CAQH CORE Connectivity Rule vC3.1.0 Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Connectivity Rule vC3.1.0. 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 submitter authentication requirement.
- 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 submitter authentication requirement.

4.3. CAQH CORE Connectivity Rule vC3.1.0 Test Scripts Assumptions

- All tests will be conducted over HTTP/S.
- The message payload is an ASC X12 Interchange.
- No editing or validation of the message payload will be performed.
- Submitter 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 submitter authentication.
- The ability to log, audit, track and report on the required data elements as required by the conformance requirements of the CAQH CORE transaction 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.

4.4. CAQH CORE Connectivity Rule vC3.1.0 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.

Connectivity										
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 SSL on communications server	Communications server accepts a valid logon by a client using X.509 Certificate		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
2	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	☐	☐	☒	☒	☒
3	On the authenticated 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 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	☐	☒	☐	☒	☒

Connectivity										
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	On an authenticated 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	☐	☐	☒	☒	☒
6	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	☐	☒	☐	☒	☒
7	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	☐	☒	☐	☒	☒
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	☐	☒	☐	☒	☒

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

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

Connectivity										
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	☐	☐	☒	☒	☒

Connectivity										
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 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 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	☐	☒	☐	☒	☒

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

6.1. 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)

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)

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

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)

6.2. 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 tests 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.

6.3. 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.

6.4. 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.

Connectivity										
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	☐	☐	☒	☒	☒

Connectivity										
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**
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	☐	☐	☒	☒	☒
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	☐	☒	☐	☒	☒