Prior Authorization & Referrals CAQH CORE Certification Test Suite
Version PA.2.0
April 2022

Revision History For Prior Authorization & Referrals 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
4.0.0	Major	Phase V CAQH CORE Certification Test Suite balloted and approved by the CAQH CORE Voting Process.	May 2019
PA.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
PA.2.0	Major	• Updated to include Test Scenarios for the CAQH CORE Attachments Prior Authorization Infrastructure Rule and CAQH CORE Attachments Prior Authorization Data Content Rule. • 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 Prior Authorization & Referrals Operating Rules to be awarded a CORE® Certification Seal. As such, this Test Suite includes:

Guidance as to the types of stakeholders to which the CAQH CORE Prior Authorization & Referrals Operating Rule Set apply and how to determine when a specific rule's detailed test script applies to a stakeholder.

- For each CAQH CORE Prior Authorization & Referrals 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 rule set, 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 an operating rule set that apply to their business and are responsible for all their own company-related testing resources. CORE Certification is available for both Real Time and Batch Processing Modes

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 CAQH CORE Pledge
3. CAQH CORE Certification Testing
4. Applying for the CORE Certification Seal

After signing the CAQH 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 signs 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., it does not include production data, volume capacity testing, all specific requirements of each rule, or end-to-end trading partner testing. CAQH CORE does not oversee trading partner relationships; CORE-certified entities may work with non-CORE-certified entities if they so desire. The CORE Certification Testing Policy is used to gain CORE Certification only; it does not outline trading partner implementation interoperability testing activities.

1.2. Eligibility For CORE Certification

[1] **CORE | CORE Certification Process | CAQH**

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. CAQH CORE Certification Testing varies based on stakeholder type; entities successfully achieving CORE Certification receive the CORE Certification Seal that corresponds with their stakeholder type.

Associations, medical societies and the like are not eligible to become CORE-certified; instead, these entities receive a CORE "Endorser" Seal after signing the CAQH CORE Pledge. Endorsers are expected to participate in CAQH CORE public relations campaigns, provide feedback and input to CAQH CORE 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 Prior Authorization & Referrals 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 CAQH 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 Participating Organizations 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 Prior Authorization & Referrals CORE Certification Testing from a CAQH CORE-authorized Testing Vendor in accordance with the Prior Authorization & Referrals CAQH CORE Certification Test Suite. This is required to maintain standard and consistent test results and CAQH CORE Prior Authorization & Referrals Operating Rule conformance. There are no exceptions to this requirement.

While the CAQH CORE Prior Authorization & Referrals Operating Rules applies 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 non 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 Clearinghouses – 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 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. Guidance for Using This CAQH CORE Certification Test Suite

[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.

2.1. Structure of Test Scenarios for the CAQH CORE Prior Authorization & Referrals Operating Rule Set

Each Test Scenario for each rule contains the following sections:

- Key Rule Requirements
  - The CAQH CORE Prior Authorization & Referrals Operating Rule Set contain 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 CORE Certification 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.

2.3. 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 Provider stakeholder type. (See §2.2.5 for more detail.)

2.4. 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, utilization management organizations (UMO), 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 Health Plan stakeholder type. (See §2.2.5 for more detail.)

2.5. 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 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 CAQH CORE Prior Authorization & Referrals Operating Rule could be considered a CORE Certification Clearinghouse stakeholder type. (See §2.2.5 for more detail.)

2.6. 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 Prior Authorization & Referrals Operating Rule). Such vendor's products or services also are eligible for CORE Certification. In the context of this Prior Authorization & Referrals CAQH CORE Certification Test Suite, a vendor with commercially-available

[3] See 45 CFR 160.103

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.)

2.7. Table of CORE Certification Stakeholder Types Examples

This table includes examples of entities that can obtain CORE Certification 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			
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[4] **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 coordinated high-quality care to their Medicare patients[5] • A network of doctors, hospital, specialists, post-acute providers and even private companies like Walgreens that shares financial and medical responsibility for	**HIPAA-covered Health Plan** Includes the following, singly or in combination:[7] • 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 • 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	**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:[8] • 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 facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity **Clearinghouse**	**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 • 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*

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

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

[7] U.S. 45 CFR 160.103

[8] Ibid.

Examples of Entities that are included in the four CORE Certification Stakeholder Types			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
providing coordinated care to patients in hopes of limiting unnecessary spending[6] • 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	• 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 individual or group plans, that provides or pays for the cost of medical care (as defined in	• An entity that brokers or mediates connectivity between a provider and a health plan either directly or through another clearinghouse • An entity that receives administrative transactions from either a provider or a health plan and forwards to the intended recipient • An entity that 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; then may disaggregate and re-aggregate transactions; and finally, route/forward the transaction to another entity.* **Health Information Exchange (Health Information Service Provider)** • An entity that provides secure transmission of clinical information between providers • An entity that provides secure t transfer of administration information between providers and health plans • An entity that provides a "community of trust" for authentication of organizations	*(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.* **Web Portal Operator** • As defined in the CAQH CORE Prior Authorization & Referrals Web Portal Operating Rule, a Web Portal Operator is any organization that makes available to either providers and their agents, payers and their agents,

[6] http://kaiserhealthnews.org/news/aco-accountable-care-organization-faq/

Examples of Entities that are included in the four CORE Certification Stakeholder Types			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
	section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)) **Utilization Management Organization (UMO)**[9] • Provides an independent, unbiased determination of medical necessity beginning with an initial clinical review, then moving to a peer clinical review if needed • Uses evidence-based treatment guidelines to enhance the quality and effectiveness of patient care while eliminating excessive treatment and expense • Understands and adheres to applicable state and federal regulations • Employs drug utilization management mechanisms to address therapeutic appropriateness, over and underutilization, dosage, duration of treatment, duplication, drug allergies, and more • Is prepared to address any risk to patient safety, such as contraindicated treatments, adverse drug interactions, or inappropriate treatment, during the review process **Third Party Administrator (TPA)**	and end users within an organization • An entity that may manage PKI digital certifications for the "community" • An entity that may transform messages to the form acceptable by the receiver • An entity that forwards clinical information to another HIE for intercommunity information exchange **Health Insurance Marketplaces or Exchanges**[10] • 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 partners), in particular enrollment information	health plans and their agents, or other organizations a web portal which supports the prior authorization process *Note: A web portal is a specially designed website that brings information from diverse sources together in a uniform way.*[12]

[9] Key functions performed by a UMO listed here are defined by URAC, a Washington DC-based non-profit organization that helps promote health care quality through the accreditation of organizations involved in medical care services.

[10] http://en.wikipedia.org/wiki/Health_insurance_marketplace

[12] https://en.wikipedia.org/wiki/Web_portal

Examples of Entities that are included in the four CORE Certification Stakeholder Types			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
	• 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[13] • 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[14] **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[15] • An arrangement in which an organization funds its own	and premium payment information **Value Added Network**[11] • 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	

[13] http://en.wikipedia.org/wiki/Third-party_administrator

[14] Ibid.

[15] http://en.termwiki.com/EN/administrative_services_only_(ASO)_contract

[11] http://en.wikipedia.org/wiki/Value-added_network

Examples of Entities that are included in the four CORE Certification Stakeholder Types			
Provider	**Health Plan**	**Clearinghouse**	**Vendor**
	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[16] • 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[17] **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		

2.8. User Quick Start Guide

An entity can access a User Quick Start Guide specific to the set of CAQH CORE Operating Rules for which it is seeking CORE Certification when it initially establishes its testing profile on the CAQH CORE-authorized Testing Vendor's test site. The User Quick Start Guide is to be used in connection with a CAQH 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.

2.9. Guidance for Providers and Health Plans Seeking Prior Authorization & Referrals 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 Prior Authorization & Referrals Operating Rules). Thus, the Detailed Step-by-Step Test Scripts recognize that a Provider or a Health Plan may

[16] http://www.investopedia.com/terms/a/administrative-services-only.asp

[17] http://www.totalreturnannuities.com/annuity-glossary/a/administrative-services-only-aso-agreement.html

use a business associate to perform some or all the HIPAA-mandated functions required by the HIPAA-mandated standards and/or the CAQH CORE Operating Prior Authorization & Referrals Rule Set 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 must undergo CORE Certification Testing. The CAQH 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 Prior Authorization & Referrals 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 acts as a "proxy" for some of the CORE Certification requirements outlined in the Prior Authorization & Referrals CAQH CORE Certification Test Suite.

Keep in mind that certification testing differs 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 and their associated test scripts. In such a case, the Provider or the Health Plan must provide a rationale statement which explains the situation to the CAQH CORE-authorized Testing Vendor for each test script for which the N/A option is chosen and the Provider or the Health Plan needs to be prepared for a review of the rationale with CAQH CORE Staff.

2.10. CORE Master Test Bed Data

The Prior Authorization & Referrals CAQH CORE Certification Test Suite requires that all organizations seeking Prior Authorization & Referrals CORE Certification be tested using the same CORE Master Test Bed Data. The scope of the CORE Master Test Bed Data is limited to data needed for entities seeking to become Prior Authorization & Referrals CORE-certified to create and populate their internal files and/or databases addressing prior authorization only. These data are then used for internal pre-certification testing and formal Prior Authorization & Referrals CORE Certification Testing for the following CAQH CORE Prior Authorization & Referrals rule requirements:

- CAQH CORE Prior Authorization & Referrals (278) Data Content Rule
- CAQH CORE Prior Authorization & Referrals Web Portal Rule
- CAQH CORE Attachments Prior Authorization Data Content Rule

The Prior Authorization & Referrals CORE Master Test Bed Data is available at no cost to any entity in Excel spreadsheet format so that organizations may easily extract the key data elements and load them into their internal test databases. CORE Master Test Bed Data does not include all data that an entity may require to load into their internal systems; therefore, entities may need to add other data to the CORE Master Test Bed Data when loading internal systems.

The CAQH CORE-authorized testing vendor uses only the CORE Master Test Bed Data to conduct Prior Authorization & Referrals CORE Certification testing for the CAQH CORE Prior Authorization & Referrals (278) Data Content, CAQH CORE Prior Authorization & Referrals Web Portal, and CAQH CORE Attachments Prior Authorization Data Content rules.

3. CAQH CORE Prior Authorization & Referrals (278) Infrastructure Rule Test Scenario

3.1. CAQH CORE Prior Authorization & Referrals (278) 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 either Real Time Processing Mode or Batch Processing Mode.

Connectivity Requirements (§4.2)

- A HIPAA covered health plan or its agent must 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 for both Real Time and Batch Processing Modes.
- 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, §4.6)

- When an ASC X12N v5010 278 request has been submitted in Real Time Processing Mode by a HIPAA covered provider or its agent, the ASC X12N v5010 278 response must be returned with 20 seconds.
- In the case of a rejection of the ASC X12N v5010 278 Functional Group, the ASC X12C v5010 999 must be returned within the same response time.
- When an ASC X12N v5010 278 request has been submitted in Batch Processing Mode by a HIPAA covered provider or its agent by 9:00 pm Eastern Time of a business day, the ASC X12N v5010 278 response 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 Prior Authorization & Referrals (278) Infrastructure Rule Key Requirements

Use of Acknowledgements Requirements (§4.7, §4.8,)

- A HIPAA covered health plan or its agent must return an ASC X12C v5010 999 for any Functional Group of an ASC X12N v5010 278 except when it receives a Functional Group of an ASC X12N v5010 278 submitted in Real Time Processing Mode which is not rejected.
- The ASC X12C v5010 999 must report each error detected to the most specific level of detail supported by the ASC X12C v5010 999.

Companion Guide Requirements (§4.9)

- A Companion Guide covering the ASC X12N v5010 278 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 Prior Authorization & Referrals (278) Infrastructure Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the ASC X12N v5010 278 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 (except in real time), acceptance with errors (except in real time), or rejection of a Functional Group of an ASC X12N v5010 278.

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.

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 278 companion guide, and
- A copy of a page of its official ASC X12N v5010 278 companion guide depicting its conformance with the format for specifying the ASC X12N v5010 278 data content requirements.

3.2. CAQH CORE Prior Authorization & Referrals (278) Infrastructure Rule Conformance Testing 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 Prior Authorization & Referrals (278) 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 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 278 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 278 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 Prior Authorization & Referrals (278) 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 278 in either real time or batch	An ASC X12C v5010 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
5	An ASC X12C v5010 999 is not returned on an accepted ASC X12 Functional Group of an ASC X12N v5010 278 in real time	No ASC X12C v5010 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
6	An ASC X12C v5010 999 is returned on any accepted ASC X12 Functional Group of an ASC X12N v5010 278 in 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**
7	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**
8	Companion Guide conforms to the flow and format of the CORE Master Companion Guide Template	Submission of the Table of Contents of the ASC X12N v5010 278 companion guide, including an example of the ASC X12N v5010 278 content requirements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
9	Companion Guide conforms to the format for presenting each segment, data element and code flow and format of the CORE Master Companion Guide Template	Submission of a page of the ASC X12N v5010 278 companion guide depicting the presentation of segments, data elements and codes showing conformance to the required presentation format		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

4. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Test Scenario

4.1. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Key Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the CAQH CORE Prior Authorization & Referrals Operating Rule Set 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.

Provider Submission Requirements (§4.1)

- When the patient is the subscriber, the provider must submit the Patient Last Name, First Name and Date-of-Birth in Loop ID 2010C Subscriber Name NM1 and DMG segments.
- When the patient is the dependent, the provider must submit Subscriber Last Name, First Name and Date-of-Birth in Loop ID 2010C Subscriber Name NM1 and DMG segments and Dependent Last Name, First Name and Date-of-Birth in Loop ID 2010D Dependent Name NM1 and DMG segments.

Normalizing Last Name Requirements (§4.2.1, §4.2.1.1, §4.2.1.2)

- Requires a Prior Authorization & Referrals CORE-Certified health plan (or information source) to normalize the last name submitted on the 5010X217 278 and internally-stored last name prior to using submitted last name for matching or verification.

Consistent and Uniform Use of AAA Error and Action Codes Requirements (§4.2.2)

- When the health plan detects an error in data submitted in the following loops
  - Loop ID 2000A Request
  - Loop ID 2010A Utilization Management Organization (UMO) Name
  - Loop ID 2010B Requester Request
  - Loop ID 2010C Subscriber Request
  - Loop ID 2010D Dependent Request
  - Loop ID 2000E Patient Event Request
  - Loop ID 2010EA Patient Event Provider Request
  - Loop ID 2010EC Patient Event Transport Location Request
  - Loop ID 2000F Service Request
  - Loop ID 2010FA Service Provider Request

  the most specific AAA Error Code AAA03 901 Reject Reason Code permitted in the respective loops AAA Segment code set must be returned.

Out-of-network Requester, Service Provider or Specialty Entity (§4.2.2.1)

- When the requester provider, service provider or specialty entity submitted on the 5010X217 278 Request is determined to be out-of-network in the following loops
  - LOOP ID - 2010B AAA - Requester Request
  - LOOP ID - 2010EA AAA Patient Event Provider Request
  - LOOP ID - 2010FA AAA - Service Provider Request
- Error Code 35-Out of Network must be returned in AAA03 901 Reject Reason Code Data Element in addition to any other AAA03 901 Reject Reason Code

Requesting Additional Documentation for a Pended Response (§4.2.3.1)

4.1. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Key Requirements

- When the 5010X217 278 Request includes one or more Diagnosis Code(s) in Loop 2000E Patient Event Level HI Patient Diagnosis Health Care Information Codes that can be categorized by the health plan and its agent into one or more of the following types of events:
  - General Outpatient
  - Inpatient
  - Surgery
  - Oncology
  - Cardiology
  - Imaging
  - Laboratory
  - Physical Therapy
  - Occupational Therapy
  - Speech-Language Pathology

  And

  Additional medical information is required, the health plan and its agent must return data element HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review or HCR03 Industry Code 0P-Requested Information Not Received or HCR03 Industry Code 0U-Additional Patient Information Required in Loop ID 2000E HCR Health Care Services Review Segment to indicate that the review outcome is pended for additional medical information and either

  - The appropriate PWK01 Attachment Report Type Code in Loop ID 2000E PWK – Additional Patient Information Segment.

  Or

  - One or more appropriate Logical Observation Identifier Names and Codes (LOINC) Code from the HL7 CDA® R2 Attachment Implementation Guide: Exchange of C-CDA Based Documents, Release 1 (Universal Realm) Standard for Trial Use August 2017[19] in Loop ID 2000E HI – Patient Diagnosis Health Care Information Codes Segment.

  And

  - The appropriate PWK01 Attachment Report Type Code in Loop ID 2000E PWK – Additional Patient Information Segment.

Requesting Additional Documentation for a Pended Response (§4.2.3.2)

- When the 5010X217 278 Request transaction includes one or more Procedure or Revenue Code(s) in Loop 2000F Service Level SV1, SV2, or SV3 segments[20] that can be placed by the health plan and its agent into one or more of the following types of service:
  - General Outpatient
  - Inpatient
  - Surgery
  - Oncology
  - Cardiology
  - Imaging

[19] See Appendix – Section 5.3 for further description of Logical Observation Identifier Names and Codes.

[20] The 5010X217 278 Request requires the submission of a procedure or revenue code when known by the provider (requester) in Loop 2000F SV1, SV2, or SV3 Service Level Segments. When the provider needs to submit more than one procedure or revenue code Loop 2000F must be repeated for each additional code.

4.1. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Key Requirements

- Laboratory
- Physical Therapy
- Occupational Therapy
- Speech-Language Pathology

and

Additional medical information is required, the health plan and its agent must return data element HCR01 306 Action Code=A4 Pended Additional medical information is required, the health plan and its agent must return data element HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review or HCR03 Industry Code 0P-Requested Information Not Received or HCR03 Industry Code 0U-Additional Patient Information Required in Loop ID 2000F HCR Health Care Services Review Segment to indicate that the review outcome is pended for additional medical information and either

- The appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment.

Or

- One or more appropriate Logical Observation Identifier Names and Codes (LOINC) Code from the HL7 CDA® R2 Attachment Implementation Guide: Exchange of C-CDA Based Documents, Release 1 (Universal Realm) Standard for Trial Use August 2017 in Loop ID 2000F HI – Request for Additional Information Health Care Information Codes Segment.

And

- The appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment.

Using Health Care Service Decision Reason Codes (HCSDRC) (§4.2.4)

- When the health plan and its agent use the Health Care Service Decision Reason Code (HCSDRC) in Loop ID 2000E Patient Event Detail HCR Segment, if appropriate, one or more additional Health Care Service Decision Reason Codes (HCSDRC) should be returned in the HCR Segment in addition to the required code to provide the most comprehensive information to the submitter.
- When the health plan and its agent use the Health Care Service Decision Reason Code (HCSDRC) in Loop ID 2000F Service Level Detail HCR Segment, if appropriate, one or more Health Care Service Decision Reason Codes (HCSDRC) should be returned in the HCR Segment in addition to the required code to provide the most comprehensive information back to the provider.

Detection and Display of 278 Response Data Elements (§4.3)

- The receiver of a 5010X217 278 Response is required to detect and extract all data elements, data element codes and corresponding code definitions to which this rule applies as returned by the health plan and its agent in the 278 Response must display or otherwise make the data appropriately available to the end user without altering the semantic meaning of the 5010X217 278 Response data content.

4.2. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the P CAQH CORE Prior Authorization & Referrals (278) Data Content Rule. 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.

Provider Submission

The provider must submit the Patient Last Name, First Name and Date-of-Birth in Loop ID 2010C Subscriber Name NM1 and DMG segments.

The provider must submit Subscriber Last Name, First Name and Date-of-Birth in Loop ID 2010C Subscriber Name NM1 and DMG segments and Dependent Last Name, First Name and Date-of-Birth in Loop ID 2010D Dependent Name NM1 and DMG segments.

Uniform Use of AAA Error and Action Codes Requirements

The most specific AAA Error Code AAA03 901 Reject Reason Code permitted in the respective loops AAA Segment code set must be returned for errors detected in data submitted in the following loops

- Loop ID 2010B Requester Request
- Loop ID 2010C Subscriber Request
- Loop ID 2010D Dependent Request
- Loop ID 2000E Patient Event Request
- Loop ID 2000F Service Request

Requesting Additional Documentation for a Pended Patient Event Response

- To indicate that the review outcome is pended for additional medical information for a Laboratory Diagnosis Code submitted in the 5010X217 Request Loop 2000E Patient Event Level HI Patient Diagnosis Health Care Information Code the 5010X217 278 Response must include
    - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000E HCR Health Care Services Review Segment

    and

    - the appropriate PWK01 Attachment Report Type Code in Loop ID 2000E PWK – Additional Patient Information Segment.
- To indicate that the review outcome is pended for additional medical information for an Imaging Diagnosis Code submitted in the 5010X217 Request Loop 2000E Patient Event Level HI Patient Diagnosis Health Care Information Code the 5010X217 278 Response must include
    - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000E HCR Health Care Services Review Segment

    and

    - the appropriate PWK01 Attachment Report Type Code in Loop ID 2000E PWK – Additional Patient Information Segment.
- To indicate that the review outcome is pended for additional medical information for a Cardiology Diagnosis Code submitted in the 5010X217 278 Request Loop 2000E Patient Event Level HI Patient Diagnosis Health Care Information Code the 5010X217 278 Response must include
    - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000E HCR Health Care Services Review Segment

    and

4.2. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Conformance Testing Requirements

- one appropriate Logical Observation Identifier Names and Codes (LOINC) Code in data element 2017 in Loop ID 2000E HI – Patient Diagnosis Health Care Information Codes Segment

and

- the appropriate PWK01 Attachment Report Type Code in Loop ID 2000E PWK – Additional Patient Information Segment.

Requesting Additional Documentation for a Pended Service Level Response

- To indicate that the review outcome is pended for additional medical information for an Imaging Procedure or Revenue Code submitted in Loop 2000F Service Level SV1 segment in the 5010X217 278 Request the 5010X217 278 Response Loop ID 2000F HCR Health Care Services Review Segment must include
  - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000F HCR Health Care Services Review Segment

  and
  - the appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment.
- To indicate that the review outcome is pended for additional medical information for an Oncology Procedure or Revenue Code submitted in Loop 2000F Service Level SV2 segment in the 5010X217 278 Request the 5010X217 278 Response Loop ID 2000F HCR Health Care Services Review Segment must include
  - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000F HCR Health Care Services Review Segment

  and
  - the appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment.
- To indicate that the review outcome is pended for additional medical information for a Laboratory Procedure or Revenue Code submitted in Loop 2000F Service Level SV1 segment in the 5010X217 278 Request the 5010X217 278 Response must include
  - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000F HCR Health Care Services Review Segment

  and
  - one appropriate Logical Observation Identifier Names and Codes (LOINC) Code in data element 2017 in Loop ID 2000F HI – Request for Additional Information Health Care Information Codes Segment

  and
  - the appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment.
- To indicate that the review outcome is pended for additional medical information for a Cardiology Procedure or Revenue Code submitted in Loop 2000F Service Level SV2 segment in the 5010X217 278 Request the 5010X217 278 Response must include
  - HCR01 306 Action Code=A4 Pended and HCR03 Industry Code 0V-Requires Medical Review in Loop ID 2000E HCR Health Care Services Review Segment

4.2. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Conformance Testing Requirements
and ○ one appropriate Logical Observation Identifier Names and Codes (LOINC) Code in data element 2017 in Loop ID 2000E HI – Patient Diagnosis Health Care Information Codes Segment and ○ the appropriate PWK01 Attachment Report Type Code in Loop ID 2000F PWK – Additional Patient Information Segment. ***Detection and Display of 278 Response Data Elements*** The receiver of a 5010X217 278 Response must detect, extract and display all data elements, data element codes and corresponding code definitions as returned in the 278 Response.

4.3. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Test Scripts Assumptions
The test scripts do not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

4.4. CAQH CORE Prior Authorization & Referrals (278) Data Content Rule Detailed Step-By-Step Test Scripts

CAQH 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 is 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 *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
Provider Request Submission & Response Processing										
1	Create a valid 5010X217 278 request transaction as defined in the CORE rule requesting a prior authorization for an Oncology service in Loop 2000F Service Level for one of the Dependents listed in the Prior Authorization & Referrals CORE Master Test Bed Data.	Output a valid fully enveloped 5010X217 278 request transaction set with complete Subscriber and Dependent names.		☐ Pass	☐ Fail	☐	☒	☐	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
2	Detect, extract, and display data elements from a valid 5010X217 278 response transaction as defined in the CORE rule using data from Test Scripts #3 through #14.	Submission of a screen print of the output from Test Scripts #3 through #14. showing that the required information is displayed to the end user.		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
AAA Error and Action Codes										
3	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying the errors detected in Loop ID 2010B Requester transaction the AAA Segment error codes.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate AAA Segment error codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
4	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying the errors detected in Loop ID 2010C Subscriber Request transaction the AAA Segment error codes.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate AAA Segment error codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
5	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying the errors detected in Loop ID 2010D Dependent Request transaction the AAA Segment error codes.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate AAA Segment error codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
6	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying the errors detected in Loop ID 2010E Patient Event Request transaction the AAA Segment error codes.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate AAA Segment error codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
7	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying the errors detected in Loop ID 2010F Service Request transaction the AAA Segment error codes.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate AAA Segment error codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
Pended Response										

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
8	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Patient Event request for Laboratory services submitted in Loop 2000E Patient Event Level is pended for additional medical information using the specified HCR segment codes and the PWK Segment to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
9	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Patient Event request for Imaging services submitted in Loop 2000E Patient Event Level is pended for additional medical information using the specified HCR segment codes and the PWK Segment to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
10	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Patient Event request for Cardiology submitted in Loop 2000E Patient Event Level is pended for additional medical information using the specified HCR segment codes and a LOINC and the PWK Segment to identify the medical information needed to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment codes and a LOINC.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
11	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Service Level request for Imaging services in Loop 2000F Services Level SV1 Segment is pended for additional medical information using the specified HCR segment codes and the PWK Segment to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
12	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Service Level request for Oncology services in Loop 2000F Services Level SV2 Segment is pended for additional medical information using the specified HCR segment codes and the PWK Segment to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
13	Create a valid 5010X217 278 response transaction as defined in the CORE rule specifying that the Service Level request for Laboratory services submitted in Loop 2000F Services Level SV1 Segment is pended for additional medical information using the specified HCR segment codes and a LOINC and the PWK Segment to identify the medical information needed to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment codes, LOINC and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
14	Create a valid 5010X217 278 response transaction as defined in the CAQH CORE rule specifying that the Service Level request for Cardiology services in Loop 2000F Services Level SV2 Segment is pended for additional medical information using the specified HCR segment codes and a LOINC and the PWK Segment to identify the medical information needed to identify the medical information needed.	Output a valid fully enveloped 5010X217 278 response transaction set with the appropriate HCR Segment codes, LOINC and PWK Segment codes.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

5. CAQH CORE Prior Authorization & Referrals Web Portal Rule Test Scenario

5.1. CAQH CORE Prior Authorization & Referrals Web Portal Rule Key Requirements

Note: This section identifies at a high level the key requirements of this rule. Refer to the CAQH CORE Prior Authorization & Referrals Operating Rule Set 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 (§4.1)

- 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.

Web Form Data Request Field Labels (§4.2.1)

- The web portal operator of prior authorization submissions must apply the corresponding loop, segment, data element name from the 5010X217 278 Request and Response to all web form data fields using the
    - IMPLEMENTATION NAME for each corresponding loop, segment and data element where an IMPLEMENTATION NAME exists

    or
    - Use the ALIAS if it is available and identified as such in the 5010X217 278 when an IMPLEMENTATION NAME does not exist or is considered less common.
- When an IMPLEMENTATION NAME or ALIAS for a corresponding loop, segment and data element does not exist the X12 base standard loop, segment and data element names must be used for the web form data field, when available.

Web Form Data Response Field Labels (§4.2.2)

- The web portal operator receiving a 5010X217 278 Response transaction to a previously submitted prior authorization request must apply the corresponding loop, segment, data element name from the 5010X217 278 Response transaction to all web form data fields using the
    - IMPLEMENTATION NAME for each corresponding loop, segment and data element where an IMPLEMENTATION NAME exists

    or
    - Use the ALIAS if it is available and identified as such in the 5010X217 278 when an IMPLEMENTATION NAME does not exist.

5.1. CAQH CORE Prior Authorization & Referrals Web Portal Rule Key Requirements

- When an IMPLEMENTATION NAME or ALIAS for a corresponding loop, segment and data element does not exist the X12 base standard loop, segment and data element names must be used for the web form data field, when available.

Use of the X12/005010X217 Health Care Services Review Request for Review and Response (278) Technical Report 3 (§4.3)

- The data collected from the web form and mapped to the X12/005010X217 Health Care Services Review – Request for Review and Response (278) transaction must comply with the CAQH CORE Prior Authorization & Referrals (278) Data Content Rule.

Confirmation of Receipt of Web Form Submission (§4.4)

- A submission receipt indicating to the provider that the completed prior authorization request form was successfully received, and the web portal operator's next steps must be returned when the submitter clicks a "submit" or similar button along with information about the web portal operator's "next steps." Examples of such information include:
    - Submitter is notified if the web portal operator requires additional documentation to process the request;
    - Submitter has the option to print and save a PDF;
    - Submitter may view the authorization status;
    - Submitter may check the status, or an update of a previously submitted request, for the prior authorization request via hypertext that includes a navigation bar or a sidebar menu linking to other web pages via hyperlinks, often referred to as links
    - Submitter is provided information about the assignment of a transaction or reference control number;
    - Submitter is provided a detailed timestamp including time zone for the submission.

5.2. CAQH CORE Prior Authorization & Referrals Web Portal Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the Web Portal rule. 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.

Web Form Data Field Labels

Display the application of the IMPLEMENTATION NAME or ALIAS to the corresponding loop, segment, data element name from the 5010X217 278 Request and Response to all web form submission data fields, when available.

5.2. CAQH CORE Prior Authorization & Referrals Web Portal Rule Conformance Testing Requirements
Use of the 005010X217 278 TR3
Demonstrate compliance with the CAQH CORE Prior Authorization & Referrals (278) Data Content Rule.
Confirmation of Web Form Submission
Demonstrate submission receipt indicating to the provider that the completed prior authorization request form was successfully received.

5.3. CAQH CORE Prior Authorization & Referrals Web Portal Rule Test Scripts Assumptions
The test scripts do not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

5.4. CAQH CORE Prior Authorization & Referrals Web Portal 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 is 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 *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
System Availability										
10	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	☐	☐	☒	☒	☒
11	Publication of non-routine downtime notice and method(s) for such publication.	Submission of a sample notice of non-routine downtime, including schedule of downtime and method(s) of publishing.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
12	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	☐	☐	☒	☒	☒
Web Form Data Field Labels										
13	Display the application of the IMPLEMENTATION NAME or ALIAS to the corresponding loop, segment, data element name from the 5010X217 278 Request and Response to all web form submission data fields.	Submission of actual web form showing use of Implementation Name or Alias.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
CORE Prior Authorization & Referrals (278) Data Content Rule										
14	Web portal operator must comply with CAQH CORE Prior Authorization & Referrals (278) Data Content Rule when mapping web form data collected to the 005010X217 278 transaction.	Output a valid fully enveloped 5010X217 278 request transaction set.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
Confirmation of Web Form Submission										

Test #	Criteria	Expected Result	Actual Result	Pass	Fail	N/A	Stakeholder *An X in the box indicates the stakeholder type to which the test applies*			
							Provider	Health Plan	Clearinghouse	Vendor
15	Display the submission receipt of the web form submission data fields.	Submission of actual web page confirming successful receipt of the request.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

6. CAQH CORE Attachments Prior Authorization Infrastructure Rule Test Scenario

6.1. CAQH CORE Attachments Prior Authorization 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.

Infrastructure Rule Requirements for Attachments using the X12 275 Transaction

Processing Mode Requirements for X12 275 Attachments (§4.1)

- A HIPAA covered health plan and its agent must implement server requirements for Batch Processing Mode **OR** Real Time Processing Mode.

Connectivity Requirements for X12 275 Attachments (§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 for X12 275 Attachments for X12 275 Attachments (§4.3)

- A HIPAA covered health plan and its agent's system availability must be no less than 90 percent per calendar week for both Real Time and Batch Processing Modes.
- 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 and its agent must publish their regularly scheduled system downtime in an appropriate manner.
- A HIPAA covered health plan and its agent must publish the schedule of non-routine downtime at least one week in advance.
- A HIPAA covered health plan and 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 and its agent must establish and publish its own holiday schedule.

Payload Acknowledgements and Response Time for X12 275 Attachments (§4.4)

- When any Functional Group of an X12 v6020X316 275 Attachment Transaction Set is accepted, accepted with errors, or rejected the HIPAA-covered health plan and its agent must return a X12 v6020X290 999 transaction.
- The X12 v6020X290 999 transaction must report each error detected to the most specific level of detail supported by the X12 v6020X290 999.
- 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.

6.1. CAQH CORE Attachments Prior Authorization Infrastructure Rule Key Requirements

- When an X12 v6020X316 275 has been submitted by a HIPAA covered provider and its agent in Batch Processing Mode, by 9:00 pm Eastern Time of a business day, an X12 v6020X290 999 must be available for pick up by 7:00 am Eastern Time on the second business day following submission.
- When an X12 v6020X316 275 has been submitted by a HIPAA covered provider or its agent in Real Time Processing Mode, the maximum response time for the receipt of an X12 v6020X290 999 must be 20 seconds.
- The receiver of an X12 v6020X290 999 must:
    - Process any X12 v6020X290 999 within one business day of its receipt, and
    - Recognize all error conditions that can be specified using all standard acknowledgements named in this rule, and
    - Pass all such error conditions to the end user as appropriate

      Or
    - Display to the end user text that uniquely describes the specific error condition(s).

Data Handling Requirements for X12 275 Attachments (§4.5)

- At the Payload Processing Layer, the receiver of an X12 v6020X316 275 must return an X12 v6020X290 999 to notify providers and their agents (submitter/client) of the acceptance, acceptance with error, or rejection.
- At the Initial Data Content Processing Layer, if the receiver (server) responds, it must also return an X12 v6020X257 824 to notify providers and their agents (submitter/client) of the acceptance, acceptance with error, or rejection of the X12 v6020X316 275 transaction and the content of the Binary Data Segment (BDS) segment in the X12 v6020X316 275 in addition to the X12 v6020X290 999 and the X12 v5010X217 278 Response.
- A receiver of an X12 v6020X257 824 must return an X12 v6020X290 999 for each Functional Group of X12 v6020X257 824 to indicate that the that it was either accepted, accepted with errors or rejected.

File Size Requirements for X12 275 Attachments (§4.6)

- A HIPAA-covered entity and its agent must be able to accept a Minimum 64MB of Base64 encoded data by their front-end servers when the encoded data received is exchanged via the X12 v6020X316 275.
- A HIPAA-covered entity and its agent must be able to accept a Minimum 64MB file size document by their internal document management systems used for holding and processing attachments.

Companion Guide Requirements for X12 275 Attachments (§4.7)

- A Companion Guide covering the X12 v6020X316 275 published by a HIPAA covered health plan and its agent must follow the format/flow as defined in the CAQH CORE Master Companion Guide Template.

<u>Infrastructure Rule Requirements for Additional Documentation using the Non-X12 Method</u>
Connectivity Requirements for Additional Documentation using CORE Connectivity using the Non-X12 Method (§5.1)

6.1. CAQH CORE Attachments Prior Authorization Infrastructure Rule Key Requirements

- If a HIPAA-covered entity and its agent elect to use CORE Connectivity as their non-X12 method of additional documentation submission, the most recent published and CAQH CORE adopted version of the CAQH CORE Connectivity Rule must be supported.

System Availability and Reporting Requirements for Additional Documentation using the Non-X12 Method (§5.2)

- A HIPAA covered health plan and its agent's system availability must be no less than 90 percent per calendar week for both Real Time and Batch Processing Modes.
- 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 and its agent must publish their regularly scheduled system downtime in an appropriate manner.
- A HIPAA covered health plan and its agent must publish the schedule of non-routine downtime at least one week in advance.
- A HIPAA covered health plan and 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 and its agent must establish and publish its own holiday schedule.

File Size Requirements for Additional Documentation using the Non-X12 Method (§5.3)

- A HIPAA-covered entity and its agent must be able to accept a Minimum 64MB of Base64 encoded data by their front-end servers when the encoded data received is exchanged via a non-X12 method.
- A HIPAA-covered entity and its agent must be able to accept a Minimum 64MB file size document by their internal document management systems used for holding and processing attachments.

6.2. CAQH CORE Attachments Prior Authorization Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Attachments (275/278) Prior Authorization Infrastructure Rule. 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 for X12 275 Attachments and Non-X12 Methods:

- 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 X12 v6020X290 999 is returned to indicate either acceptance, acceptance with errors, or rejection a Functional Group of an X12 v6020X316 275 attachment transaction set when the ASC X12N v6020X316 275 is submitted in batch processing mode.
- An X12 v6020X290 999 is returned to indicate rejection only when the ASC X12N v6020X316 275 submitted in real time is rejected.

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.

Data Handling

- An X12 v6020X257 824 is returned to indicate either acceptance, acceptance with errors, or rejection of the X12 v6020X316 275 transaction and the content of the Binary Data Segment (BDS) segment.
- An X12 v6020X290 999 is returned to indicate either acceptance, acceptance with errors, or rejection for each Functional Group of an X12 v6020X257 824.

File Size

- Demonstrate the ability to accept a Minimum 64MB file size attachment by front-end servers and internal document management systems for X12 275 Attachments and Non-X12 Methods.

Companion Guide

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

6.2. CAQH CORE Attachments Prior Authorization Rule Conformance Testing Requirements
• A copy of the table of contents of its official X12 v6020X316 275 companion guide. • A copy of a page of its official X12 v6020X316 275 companion guide depicting its conformance with the format for specifying the X12 v6020X316 275 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.

6.3. CAQH CORE Attachments Prior Authorization 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 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 X12 interchange containing the X12 v6020X290 999 and X12 v6020X257 824 transactions. • The detailed content of the companion guide will not be submitted to the CORE-authorized Testing Vendor. • The detailed content of the companion guide will not be examined nor evaluated.

6.4. CAQH CORE Attachments Prior Authorization 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 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 for X12 275 Attachments										
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**
15	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	☐	☐	☒	☒	☒
16	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	☐	☐	☒	☒	☒
17	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 for X12 275 Attachments										
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**
18	An X12 v6020X290 999 is returned on a rejected X12 Functional Group of ASC X12N v6020X316 275 in either real time or batch	An X12 v6020X290 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
19	An X12 v6020X290 999 is not returned on an accepted X12 Functional Group of an X12N v6020X316 275 in real time	No X12 v6020X290 999 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
20	An X12 v6020X290 999 is returned on any accepted ASC X12 Functional Group of an X12N v6020X316 275 in batch	An X12 v6020X290 999 is returned on any accepted ASC X12 Functional Group of an X12N v6020X316 275 in batch		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Response Time for X12 275 Attachments										
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**
21	Verify that outer most communications module(s) transmit 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 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 a system-generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Data Handling for X12 275 Attachments										
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**
22	An X12 v6020X257 824 is returned on a rejected X12 Functional Group of an X12N v6020X316 275 in either real time or batch.	An X12 v6020X257 824 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
23	An X12 v6020X257 824 is returned on an accepted X12 Functional Group of an X12N v6020X316 275 in either real time or batch.	An X12 v6020X257 824 is returned		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
24	An X12 v6020X290 999 is returned on a rejected X12 Functional Group of a X12 v6020X257 824.	An X12 v6020X290 999 is returned		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
25	An X12 v6020X290 999 is returned on an accepted X12 Functional Group of an X12 v6020X257 824.	An X12 v6020X290 999 is returned		☐ Pass	☐ Fail	☐	☒	☐	☒	☒

File Size for X12 275 Attachments										
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**
26	Verify that front-end servers support the ability to accept a minimum of 64MB file size attachments.	Submission of screenshot of file size limitation policies.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
27	Verify that internal document manage systems support the ability to accept a minimum of 64MB file size attachments.	Submission of screenshot of file size limitation policies.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Companion Guide for X12 275 Attachments										
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**
28	Companion Guide conforms to the flow and format of the CAQH CORE Master Companion Guide Template	Submission of the Table of Contents of the 275 companion guide, including an example of the X12N v6020X316 275 content requirements		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
29	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 X12N v6020X316 275 companion guide depicting the presentation of segments, data elements and codes showing conformance to the required presentation format		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

System Availability for Non-X12 Methods										
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**
30	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	☐	☐	☒	☒	☒
31	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	☐	☐	☒	☒	☒
32	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	☐	☐	☒	☒	☒

File Size for Non-X12 Methods										
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**
33	Verify that front-end servers support the ability to accept a minimum of 64MB file size attachments.	Submission of screenshot of file size limitation policies.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒
34	Verify that internal document management systems support the ability to accept a minimum of 64MB file size attachments.	Submission of screenshot of file size limitation policies.		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

7. CAQH CORE Attachments Prior Authorization Rule Data Content Rule Test Scenario

7.1. CAQH CORE Attachments Prior Authorization Rule Data Content 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.

Reassociation Requirements for X12 Methods (§4.1)

- When a HIPAA-covered provider and its agent send an unsolicited X12 v6020X316 275 in support of an X12 v5010X217 278, PWK02 Code EL in Loop 2000E/Loop 2000F in the X12 v5010X217 278 Request must be used to notify a HIPAA-covered health plan and its agent that additional documentation is being transmitted electronically using the Binary Data Segment (BDS) in X12 v6020X316 275.
- When a provider sends a X12 v6020X316 275 to support an X12 v5010X217 278 Prior Authorization Request, CAQH CORE recommends the use of the common reference data to be included on the X12 v6020X316 275 for patient identification and reassociation purposes.
- A HIPAA-covered health plan and its agent must use PWK02 Code EL in Loop 2000E/Loop 2000F in a pended X12 5010X217 278 Response to request the electronic submission of additional documentation supporting medical necessity in the X12 v6020X316 275.

Reassociation Requirements for Non-X12 Methods (5.1)

- When sending a non-X12 unsolicited attachment using CORE SOAP Connectivity Requirements §4.4.3 <SDO>_<PayloadType>_<Version>_<Sub-version> the provider and its agent may identify the <PayloadType> as specified.
- When sending a non-X12 unsolicited attachment using CORE REST Connectivity Requirements §5.3.2 Specifications for REST API URI Path Endpoints for Payload Types the provider and its agent may identify the REST API URI Path Endpoint as specified.
- A provider and its agent must include all available Attachment Data Elements as part of the attachment payload when sending additional information to ensure reassociation with the prior authorization.

7.2. CAQH CORE Attachments Prior Authorization Data Content Rule Conformance Testing Requirements

These scenarios test the following conformance requirements of the CAQH CORE Attachments (275/278) Prior Authorization Rule Data Content Rule. 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.

Reassociation Requirements for X12 Methods

- Demonstrate ability to support necessary data elements in order to support the reassociation of an X12 v6020X316 275 to an X12 v5010X217 278.
- Demonstrate the ability to reassociate an X12 v6020X316 275 to a an X12 v5010X217 278.

Reassociation Requirements for Non-X12 Methods

- Demonstrate the ability to reassociate a non X12 attachment to an X12 v5010X217 278 using CORE SOAP Connectivity.
- Demonstrate the ability to reassociate a non X12 attachment to an X12 v5010X217 278 using CORE REST Connectivity.
- Demonstrate the ability to include all available Attachment Data Elements as part of the attachment payload when sending additional information.

7.3. CAQH CORE Attachments Prior Authorization Data Content Rule Test Scripts Assumptions

- The test scripts will not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

7.4. CAQH CORE Attachments Prior Authorization Data Content 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 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.

Reassociation of X12 275 Attachments										
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**
35	Create a valid X12 v5010X217 278 Request, specifying PWK02 Code EL in Loop 2000E/2000F	Output a valid X12 v5010X217 278 Request containing PWK02 Code EL in Loop 2000E/2000F		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
36	A provider's system must be able to support the inclusion of the CAQH CORE common reference data on the X12 v6020X316 275 for patient identification and reassociation purposes in support an X12 v5010X217 278 Request	Provide a screen print of the output of a X12 v6020X316 275 showing the inclusion of the CAQH CORE common reference data		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
37	Create a valid X12 v5010X217 278 Response specifying	Output a valid X12 v5010X217 278 Response containing		☐ Pass	☐ Fail	☐	☐	☒	☒	☒

Reassociation of X12 275 Attachments										
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**
	PWK02 Code EL in Loop 2000E/Loop 2000F	PWK02 Code EL in Loop 2000E/2000F								

Reassociation of Non-X12 Methods										
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**
38	Verify that communications **client** creates, assigns, logs, links the required metadata elements to message payload using CORE SOAP Connectivity	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
39	Verify that communications **client** creates, assigns, logs, links the required metadata elements to message payload using CORE REST Connectivity	Output a system generated audit log report showing all required data elements		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
40	A provider's system must be able to support the inclusion of the CAQH CORE Attachment Data Elements on non-X12 attachment payloads for patient identification and reassociation purposes in support a prior authorization.	Provide a screen print of the output of a non-X12 attachment payload showing the inclusion of CAQH CORE Attachment Data Elements		☐ Pass	☐ Fail	☐	☒	☐	☒	☒

8. CAQH CORE Connectivity Rule vC3.1.0 Test Scenario

8.1. 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).

8.2. 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.

8.3. 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.

8.4. 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	☐	☐	☒	☒	☒

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 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	☐	☒	☐	☒	☒
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	☐	☒	☐	☒	☒

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**
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	☐	☒	☐	☒	☒

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

9.1. 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.

9.2. 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.

9.3. 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.

9.4. 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
10	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	☐	☐	☒	☒	☒
11	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	☐	☐	☒	☒	☒
12	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	☐	☐	☒	☒	☒
13	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**
14	Implement X.509 certificate authentication method as a communications client	Client successfully logs on to a communications server with X.509 certificate		☐ Pass	☐ Fail	☐	☒	☐	☒	☒
15	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	☐	☒	☐	☒	☒
16	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	☐	☒	☐	☒	☒
17	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	☐	☐	☒	☒	☒
18	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	☐	☒	☐	☒	☒

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

10.1. 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)

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

- 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)

10.2. 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.

10.3. 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.

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

- The CORE test scripts will not include comprehensive testing requirements to test for all possible permutations of the CORE requirements of the rule.

10.4. 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	☐	☒	☐	☒	☒