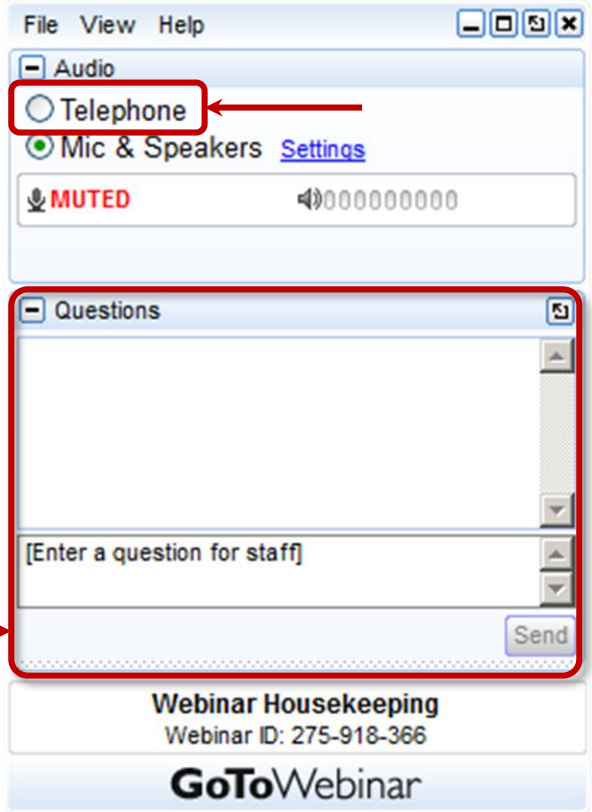
CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Wednesday,
February 24th, 2016
2:00 – 3:00 PM ET

Logistics
How to Participate in Today's Session

- Download a copy of today's presentation on the CAQH.org website
  - Navigate to the CORE Education Events page and access a pdf version of today's presentation under the list for today's event
- The phones will be muted upon entry and during the presentation portion of the session
- At any time throughout the session, you may communicate a question via the web
  - Questions can be submitted ***at any time*** with the **Questions panel on the right side of the GoToWebinar desktop**



CAQH CORE

Session Outline

- Background on the Phase IV CAQH CORE 470 Connectivity Rule
- Key Technical Concepts
  - Problem Description
  - Scope and Applicability
- Technical Requirements
  - Envelope Requirements
  - Security Requirements
  - Payload Processing Mode Requirements
  - Message Interactions
  - Conformance Requirements for Stakeholders
- CAQH CORE Resources for Implementers
- Q&A/Commonly Asked Questions
- Appendix

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Overview

Purpose

- This presentation will provide technical details and review the requirements for implementing the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Audience

- The intended audience consists of technical implementers of CAQH CORE Connectivity Rules for Claims, Prior Authorizations, Benefit Enrollment and Premium Payment transactions in your organization

Prerequisites

- Basic understanding of CAQH CORE mission, vision and Guiding Principles; click HERE for an overview
- Conceptual understanding of Connectivity Rules that are part of the federally mandated Operating Rules set. CAQH CORE general background information is available by clicking HERE
- Working knowledge of technical concepts such as client/server connectivity and SOAP+WSDL, X.509 Digital Certificates, SSL and TLS

Required Materials

- This PowerPoint and a copy of the CAQH CORE Connectivity Operating Rules for reference
  - Phase II Connectivity Rule click HERE
  - Phase IV Connectivity Rule, click HERE

Background on the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Robert Bowman
CAQH CORE Senior Manager

ACA Mandated Operating Rules and Certification *Compliance Dates*

Phases I-II COMPLIANCE	Phase III COMPLIANCE	ACA-Mandated HHS Health Plan Certification	Phase IV
January 1, 2013	**January 1, 2014**	**TBD**	**TBD**
Health plan eligibility **Claim status transactions** *HIPAA covered entities conduct these transactions using the CAQH CORE Operating Rules*	**Electronic funds transfer (EFT)** **Health care payment and remittance advice (ERA)** *HIPAA covered entities conduct these transactions using the CAQH CORE Operating Rules*	**ACA mandates health plans must certify to HHS compliance with Eligibility/ Claim Status/ EFT/ERA operating rules and underlying standards** *Applies only to health plans and includes potential penalties for incomplete certification*	**Health claims or equivalent encounter information** **Referral, certification and authorization** **Enrollment/ disenrollment in a health plan** **Health plan premium payments** **Health claims attachments (HHS Standard not yet mandated)**
Mandated Requirements	**Mandated Requirements**	**New HHS proposed rule expected April, 2016**	**Phase IV Op Rules approved for voluntary implementation by CAQH CORE Part Org and CORE Board**

CAQH CORE

Phase IV CAQH CORE Operating Rules
Regulatory Next Steps

NCVHS

CAQH CORE updated NCVHS on the status of the Phase IV Operating Rules

(earlier hearing and letter)

CAQH CORE testified before NCVHS Review Committee on the Phase IV CAQH CORE Operating Rules on February 16, 2016

As appropriate, NCVHS could make an adoption recommendation to the HHS Secretary

HHS

HHS may publish a regulation in the Federal Register once it determines what is appropriate for Federal mandate

A public comment period (60 days or more) would follow publication of any regulation whereby entities can submit comments on the regulation to CMS/HHS

Industry

Based on public comments to the regulation, industry will be required to implement the operating rules, usually within two years of publication of a final regulation

Public Comment Opportunity

CAQH CORE

Scope of Phase IV CAQH CORE Rule Requirements

Reminder: Health Claims Attachments transaction not included; there is no formal HIPAA Health Claims Attachments standard(s).

Infrastructure Requirement	Prior Authorization	Claims	Enrollment/ Disenrollment	Premium Payment
Processing Mode	*Batch OR Real Time Required*	*Batch Required; Real Time Optional*	*Batch Required; Real Time Optional*	*Batch Required; Real Time Optional*
Batch Processing Mode Response Time	*If Batch Offered*	**X**	**X**	**X**
Batch Acknowledgements	*If Batch Offered*	**X**	**X**	**X**
Real Time Processing Mode Response Time	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*
Real Time Acknowledgements	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*	*If Real Time Offered*
Safe Harbor Connectivity and Security	**X**	**X**	**X**	**X**
System Availability	**X**	**X**	**X**	**X**
Companion Guide Template	**X**	**X**	**X**	**X**
Other	N/A	Include guidance for COB in companion guide	Timeframe requirements to process data after successful receipt and verification of transaction	Timeframe requirements to process data after successful receipt and verification of transaction

X = Required

CAQH CORE

Complete Set of Phase IV CAQH CORE Operating Rules

Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule v4.0.0

Phase IV CAQH CORE 452 Health Care Services Review – Request for Review and Response (278) Infrastructure Rule v4.0.0

Phase IV CAQH CORE 454 Benefit Enrollment and Maintenance (834) Infrastructure Rule v4.0.0

Phase IV CAQH CORE 456 Premium Payment (820) Infrastructure Rule v4.0.0

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Focus of This Presentation

CAQH CORE

Phase IV CAQH CORE Connectivity Rule v4.0.0
Development Philosophy

Based on CAQH CORE Mission and Vision of improving administrative simplification through operational uniformity and interoperability

- Developed by industry using a consensus-based approach

Consistent with CORE Guiding Principles; e.g.,

- Builds on existing standards (e.g., HTTP/S, SOAP, MTOM, SSL/TLS)
- Aligns with national initiatives in healthcare information exchange, including clinical domain

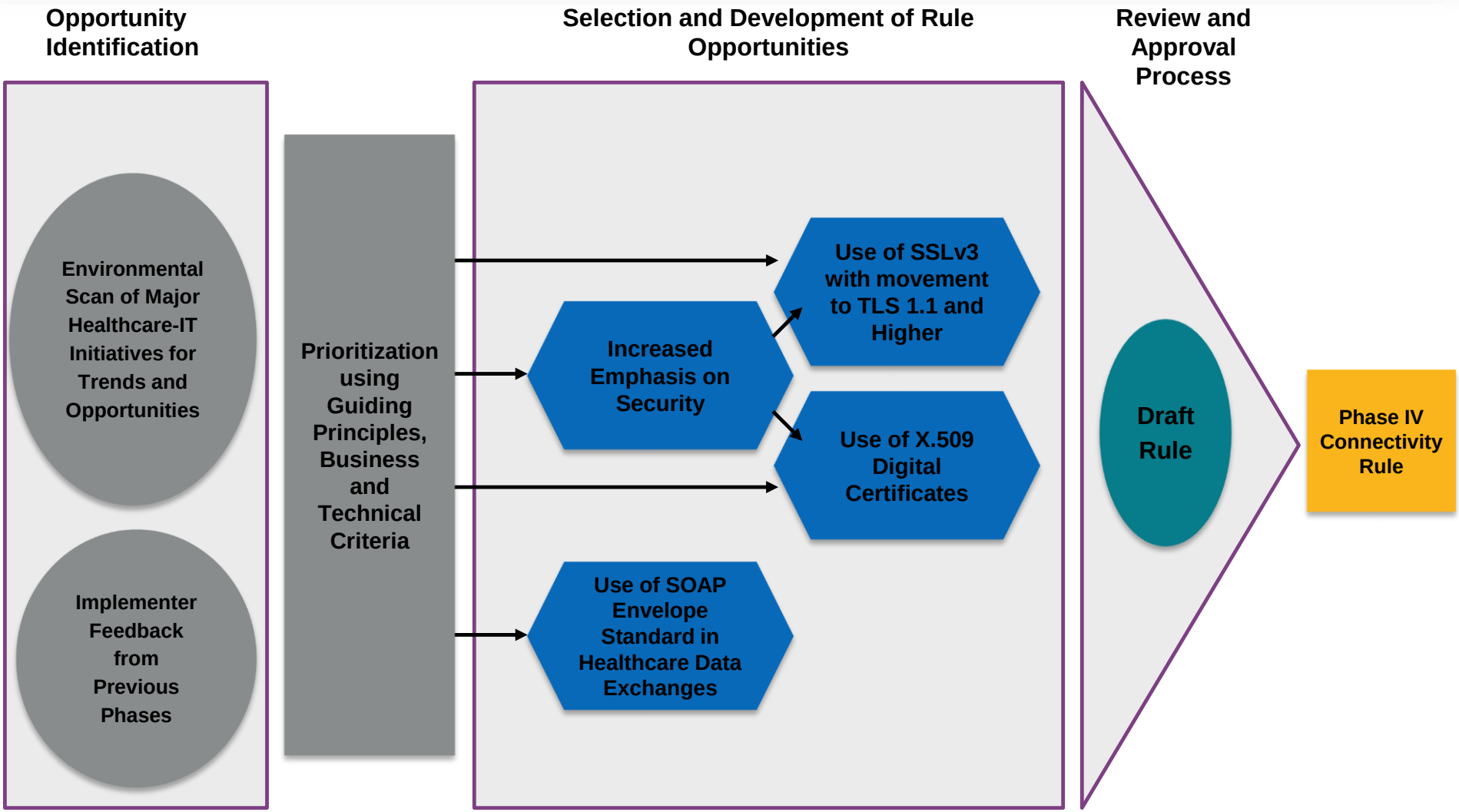
Consistent with CORE Connectivity technical and security principles; e.g.,

- Payload agnostic
- Language and platform neutral
- Supports real-time and batch transactions
- Safe Harbor Connectivity

Developed based on

- Foundation established by previous CORE Connectivity phases
- Implementer feedback from previous phases
- Industry-wide environmental scan
- Extensive list of evaluation criteria

Phase IV CAQH CORE Connectivity Rule *Development Process*



CAQH CORE Connectivity Rule Phases & Applicability to *ASC X12 Transactions*

Each Phase Builds on Previous Phases

- **Claims**
- **Prior Authorizations**
- **Benefit Enrollments**
- **Premium Payments**

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 (Safe Harbor)

- Convergence on single Message Envelope Standard for both Real Time and Batch Processing
- Convergence on single Submitter Authentication Standard
- Improved Transport Security
- Enhancement of Message Interactions for Supporting New Transactions

- **Eligibility**
- **Claim Status**
- **Electronic Remittance Advice**

Phase II CAQH CORE 270 Connectivity Rule v2.2.0 (Safe Harbor)

- Definition of Message Metadata
- Selection of two Message Envelope Standards
- Selection of two Submitter Authentication Standards
- Selection of Transport Security Standards
- Specification of Message Interactions

- **Eligibility**
- **Claim Status**

Phase I CAQH CORE 153 Connectivity Rule v1.0.0

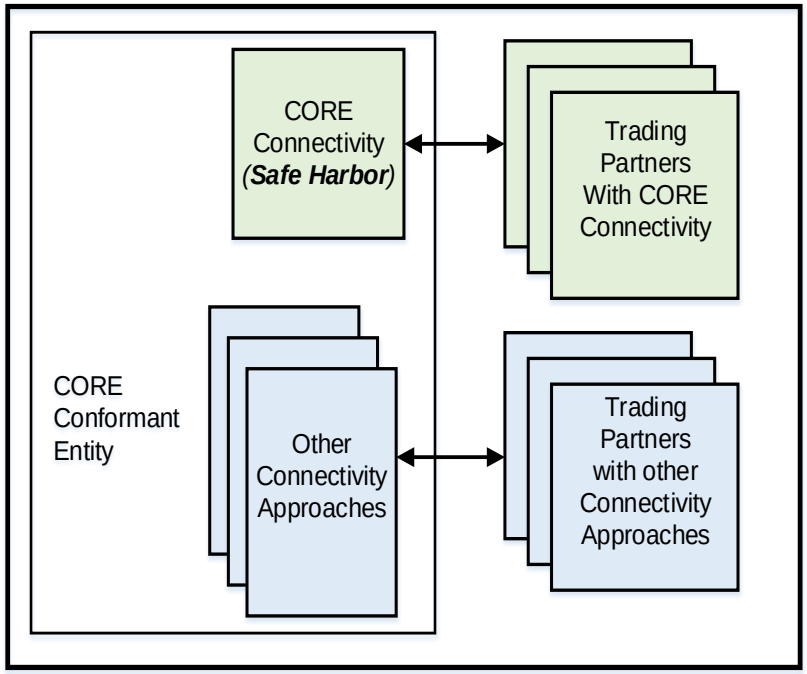
- Use of Public Internet and HTTP/S

CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
CORE Safe Harbor Principle

The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 is the "CORE Safe Harbor" connectivity method that a HIPAA covered entity or its agent must implement, and **MUST use if requested by a trading partner**

- Trading partners always have systems that are interoperable between them



Enables trading partners to use different communications and security methods than what is specified in rule:

- HIPAA covered entities must support CAQH CORE Operating Rule requirements for real time and batch processing modes
  - Can offer other communications and security methods
  - Does not require trading partners to discontinue any existing connectivity methods not conformant with CAQH CORE Operating Rules
- All message payload processing modes specified for the transactions must be supported
  - See Phase IV Connectivity Rule §4.4.3.1 and Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0

Polling Question #1: CORE Safe Harbor

Rate your understanding of the CORE Safe Harbor principle on a scale of 1-5.

1. Very Strong
2. Somewhat Strong
3. Neither strong nor weak
4. Somewhat Weak
5. Very Weak

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Key Technical Concepts

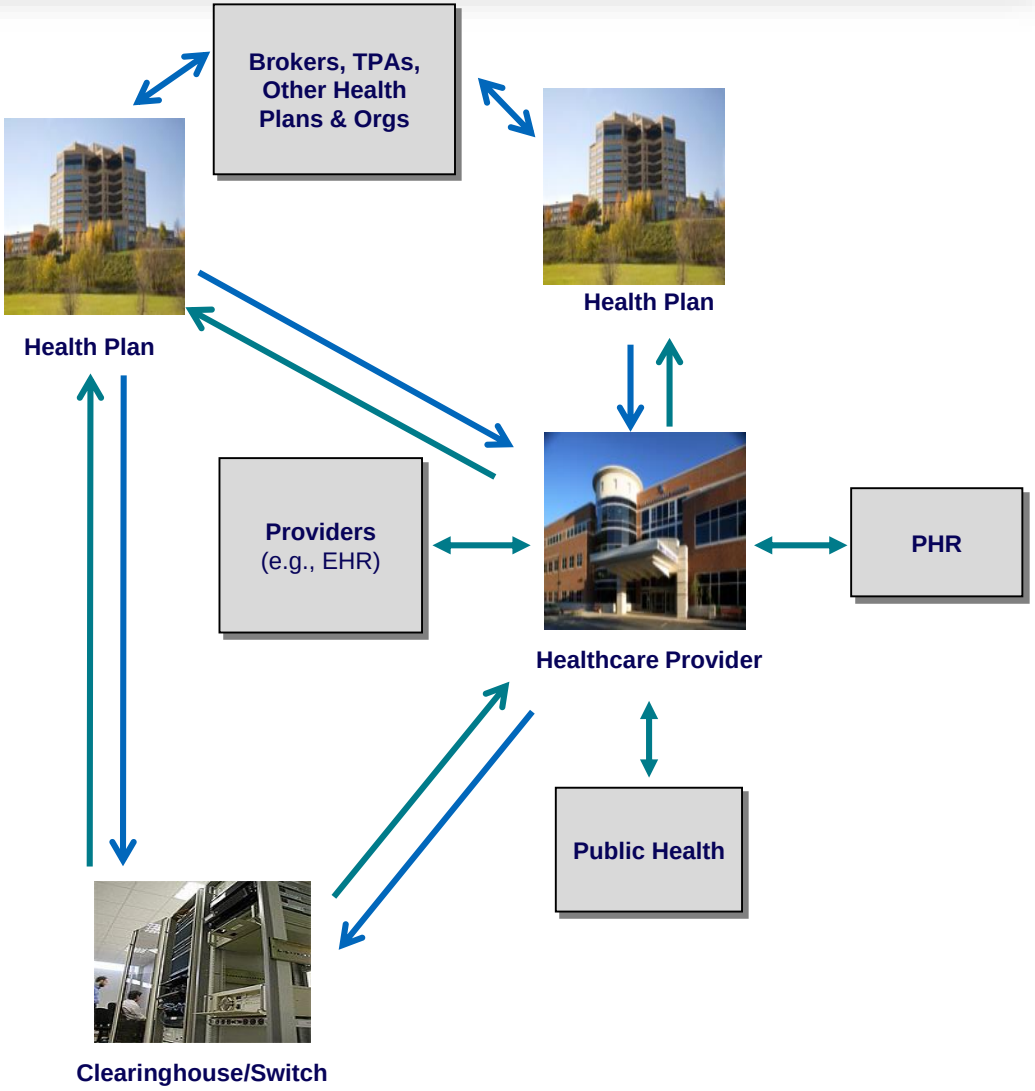
Raja Kailar
BNETAL, CEO

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 *Enhancements*

Problem: Multiple connectivity methods are utilized across the industry

- Various connectivity methods for exchanging Claims, Prior Authorization, Benefit Enrollments and Premium Payment transactions both manually and/or electronically drive elevated transaction costs and increase operational complexity

Solution: Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 **enhances interoperability, efficiency and security by defining technical requirements** for the exchange of the above electronic transactions between trading partners; entities can be assured of a common connectivity method



Applicability of Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Using the Internet as a delivery option, establishes a Safe Harbor connectivity method that application vendors, providers, and health plans can be assured will be supported by any HIPAA covered entity, meaning that the entity is capable and ready at the time of a request by a trading partner to exchange data using the Phase IV CAQH CORE Connectivity Rule

- Phase IV Connectivity Rule builds on Phase II Connectivity Rule to include more prescriptive submitter authentication, envelope specifications, etc.
- CORE Safe Harbor applies when an entity conducts Claims, Prior Authorization, Benefit Enrollments and Premium Payment transactions

Applies to information sources performing the role of an HTTP/S server and information receivers performing the role of an HTTP/S client

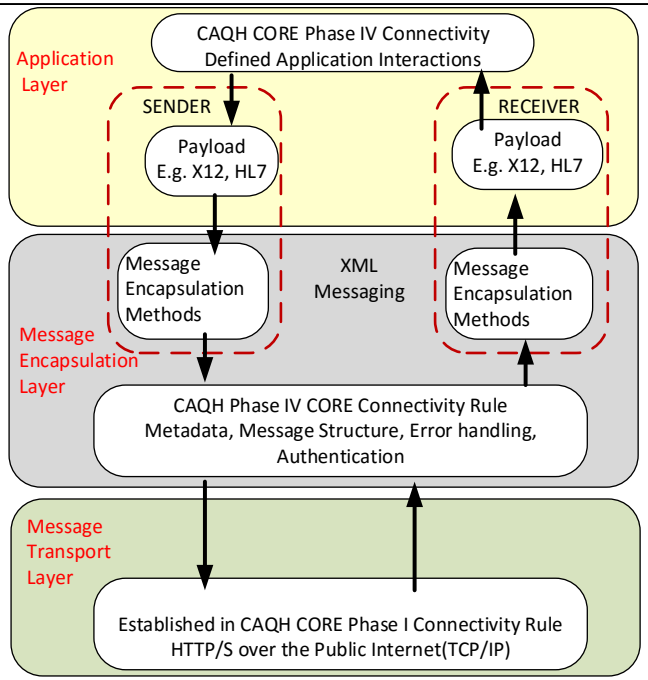
- Applies to both batch and real time transactions
- Does not require trading partners to remove existing connections that do not match the rules

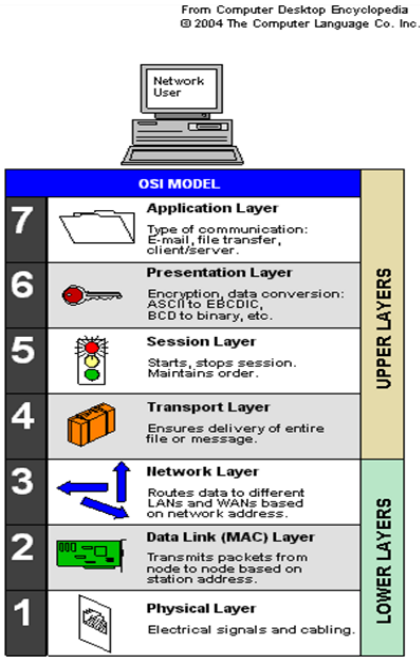
Technical Scope
What the Rule Applies To – OSI Model

Scope is described in terms of the network layers in the Open Systems Interconnection Basic Reference Model (OSI model) (See Rule §3.1)

The scope of the Phase IV CAQH CORE Connectivity rule is specific to:

- OSI Layers 3 and 4 (Transport and Network layers)
- OSI Layers 5 and 6 (Session and Presentation layers, also called Message Encapsulation layers)





OSI Model		Messaging Infrastructure Model
Application Layer	OSI 7	Application Layer
Presentation Layer	OSI 6	Message Encapsulation Layer (envelope)
Session Layer	OSI 5	
Transport Layer	OSI 4	Message Transport Layer
Network Layer	OSI 3	

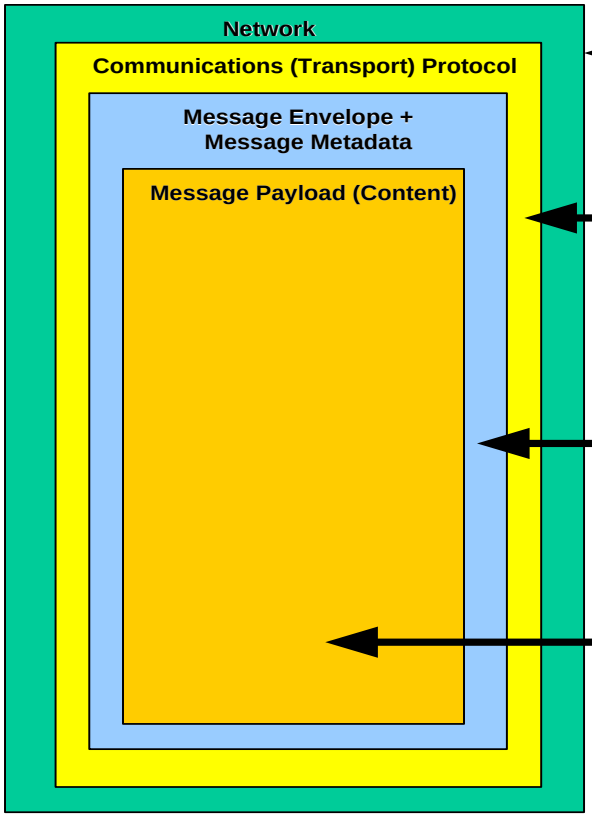
Figure Notes:

- CAQH CORE Phase IV Connectivity Rule addresses Layers 5 and 6 of the OSI Model
- Layer 3 and 4, the Transport Layer and Network Layer, was established as HTTP/S over the public internet in the CAQH CORE Phase I Connectivity Rule
- Layers 1 and 2 are not applicable to CORE because they are not items that could be included in a rule as these layers are so specific to the internal IT systems of every organization.

CAQH CORE

Technical Scope
What the Rule Applies To – Layered View

- The Message Envelope is *outside* the Message Payload (content), and *inside* the Transport Protocol envelope (See Rule §3.1)
- The Transport Protocol Envelope corresponds to OSI Model Layer 3 and 4
- The Message Envelope corresponds to OSI Model Layers 5 and 6
- The Message Payload (content) corresponds to OSI Model Layer 7



= Public Internet (TCP/IP) - established in CAQH CORE Phase I Connectivity

= HTTP over SSL 3.0, or optionally TLS 1.1 or higher. (HIPAA covered entities that wish to use stronger security or must also be FIPS 140-2 compliant may implement TLS 1.1 or higher in lieu of SSL 3.0)

= Message Envelope & Message Metadata (SOAP + MTOM) – CAQH CORE Phase IV Connectivity

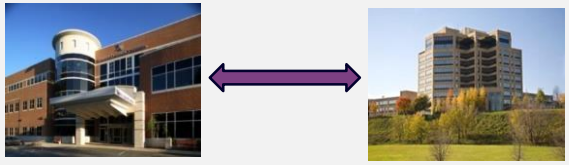
= HIPAA Administrative Transactions (X12)
HL7 Clinical Messages
Zipped Files
Personal Health Record
Other Content

Technical Scope
What the Rule Applies To – Business to Business Connection Models

Interoperability and efficiency is enhanced by the Phase IV CAQH CORE Connectivity Rule's defined technical requirements for exchange of administrative transactions between trading partners, also known as a Business to Business (B2B) relationship

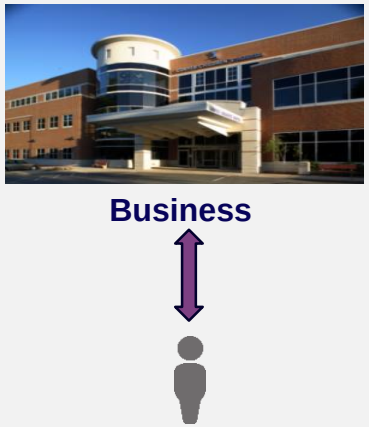
- The Connectivity Rule can be applied independently of the communication architecture or model (e.g., two models are shown below)
- The Connectivity Rule <u>does not</u> apply to Direct Data Entry (DDE) systems

Model 1: B2B Connectivity



Model 2: B2B Connectivity with Intermediary

Not Applicable: Business to Consumer Connectivity



Stakeholder Conformance Requirements
Specified in Phase IV Infrastructure Rules

The Phase IV CAQH CORE Connectivity Rule applies to health plans *(HTTP/S server)* and health care providers *(HTTP/S client)* or their agents, and Clearinghouses *(HTTP/S client)*

- The rule defines conformance requirements for stakeholders based on a typical role (client, server) for message envelope and authentication standards
- The diagram illustrates the typical *(minimal)* roles played by stakeholders (e.g., providers and submitters are typically clients, health plans and TPAs are typically servers, and clearinghouses can act as client or server)

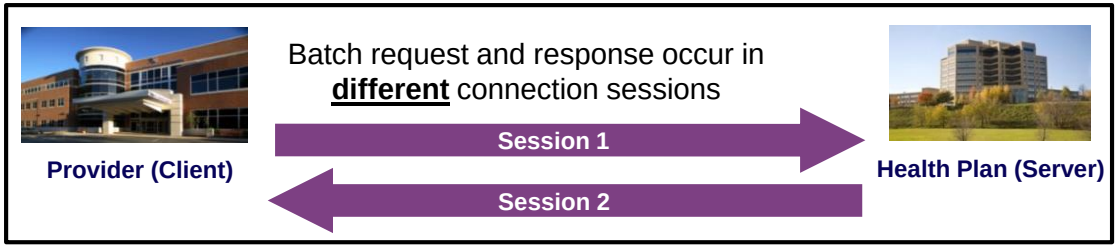
If your organization is a:	then your minimum technical role is a:
 Healthcare Provider	Client
 Clearinghouse/Switch	Client and Server
 Health Plan	Server

Technical Scope
Synchronous and Asynchronous Message Interactions/ Real Time and Batch Processing Modes

The Phase IV CAQH CORE Connectivity Rule addresses synchronous and asynchronous message interaction patterns:

- Message Interaction Patterns describe how connections are established and used for handling requests and responses

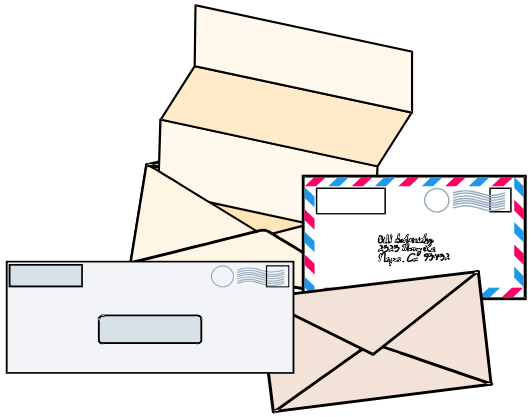
Message Interaction Patterns	Description
Synchronous	• Entity initiates a new connection to send a request; the same connection is used to receive the response for the request • Typically associated with a Real time mode of processing the message payload
Asynchronous	• Connection is established to send a request; response is sent on a separate connection • Typically associated with a Batch mode of processing the message payload



Message Encapsulation Layer
Envelopes and Metadata

The Message Envelope

- Provides a container for electronic documents (e.g., electronic claims) to be transmitted from the sender to receiver
- Keeps the contents intact, supports auditing/tracking, and provides other critical details
- Needs to include information to identify the sender/receiver (i.e., Message Envelope Metadata) and ensure documents (i.e., Message Payloads) are delivered to the receiver
- Examples of Message Payloads include the HIPAA administrative transactions (ASC X12), HL7 clinical messages and zipped files



The CORE Connectivity Rules define:

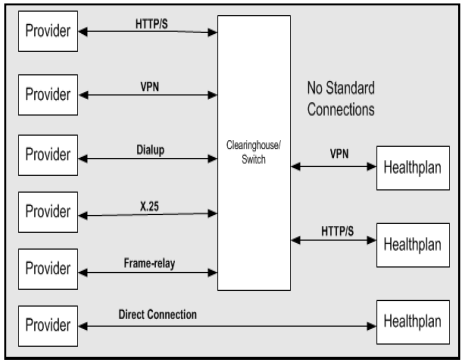
- Message Envelope and Message Envelope Metadata
  - Used primarily to conduct administrative transactions using administrative Message Payloads (e.g., ASC X12 administrative transactions)
- The Message Envelope consists of a well-defined structure for organizing and formatting Message Envelope Metadata
- The Message Envelope Metadata is normative, and helps message receivers route messages for internal processing without opening the envelope, reducing costs and improving response time
- The Message Envelope and Metadata can also be used for non administrative Message Payloads

CORE Connectivity
Moving the Industry Forward

CORE Connectivity common transport and envelope standards reduce implementation variations and improve interoperability and efficiency of administrative transactions

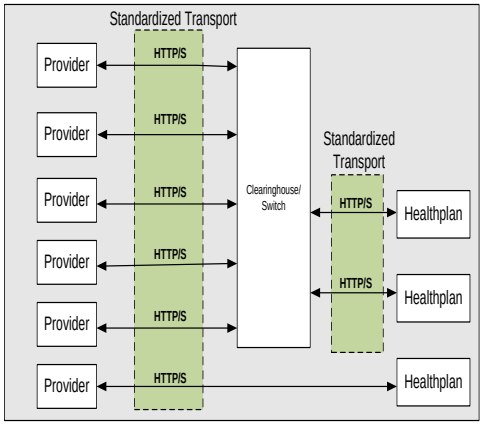
Increased interoperability and improved connectivity

Prior to CORE Connectivity: No Uniform Connection Standard



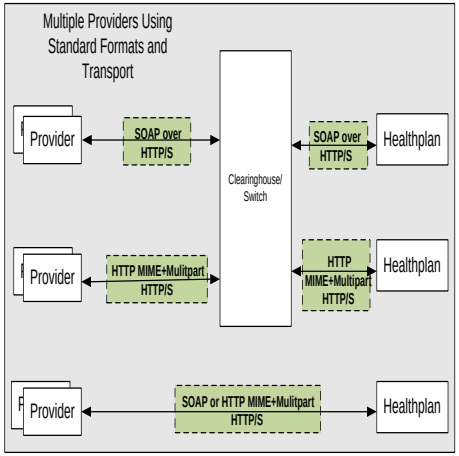
- Costly management of multiple protocols, many proprietary

Phase I CORE Connectivity: Standardized Transport



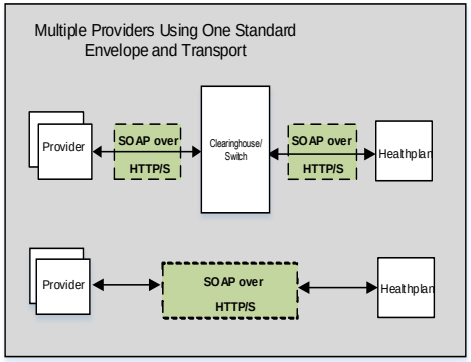
- Greater online access due to uniformity in transport protocols

Phase II CORE Connectivity: Common Transport and Envelope Standards



- Increased and less costly access due to uniformity in transport, envelope, authentication standards, and metadata
- Reduced time spent on implementations and transaction processing time

Phase IV CORE Connectivity: Single Transport & Envelope Standards



- Lower costs due to uniformity in transport, envelope, authentication standards, and metadata
- Reduced time spent on implementations and transaction processing time

CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0

Technical Requirements

Kevin Castellow
BNETAL, Senior Consultant

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Key Features

Technical Improvements

- Address Implementer Feedback to Improve Clarity
- Increased Transport Security
- Separate Payload and Processing Mode Document for Easier Maintenance
- Simplified Interoperability (Convergence to Single Envelope and Authentication Standard)
- Additional Message Interactions for Conducting New Transactions

Transaction Support

- Added Support for Claims, Premium Payments, Benefit Enrollments and Prior Authorizations
- CORE Safe Harbor allows entities to implement Phase II and/or Phase IV Connectivity for all transactions

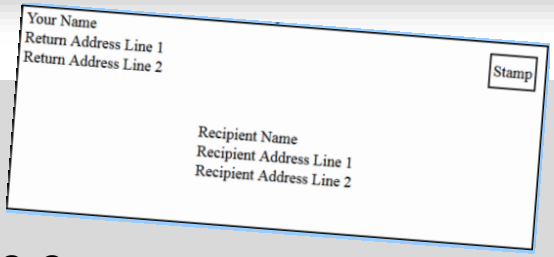
CAQH CORE Connectivity Rule Features
Detailed View & Comparison of Phases

Features	*Phase II* *CAQH CORE Connectivity Rule* *Mandated under ACA*	*Phase IV* *CAQH CORE Connectivity Rule*
Payload(s)	ASC X12 Administrative Transactions NCPDP, HL7 v2.x or v3 Messages Other	ASC X12 Administrative Transactions NCPDP, HL7 v2.x or v3 Messages Other
Submitter (Client) Authentication	Username/Password (WS-Security Token) X.509 Digital Certificate	☆ X.509 Digital Certificate over SSL v3.0/ TLS v1.1 or Higher
Message Interactions	Real Time and Batch Interactions	☆ Real Time, Batch, Generic Push and Pull Interactions
Message Envelope Metadata	CORE Specified Message Envelope Metadata	CORE Specified Message Envelope Metadata
Message Envelope(s)	MIME Multipart SOAP + WSDL	☆ SOAP + WSDL
Transport Security	Secure Sockets Layer - (SSL v3.0)	☆ Secure Sockets Layer (SSLv3.0 with optional use of TLS1.1 or higher. Entities needing higher security can use TLS1.1 in lieu of SSLv3.0)
Transport Layer	HTTP over TCP	HTTP over TCP
Network	Public Internet	Public Internet

☆ Revised from Phase II

CAQH CORE

Message Transport Layer: *Envelope Standard*



SOAP+WSDL

- The Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 supports one envelope standard to attach and send files
- SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information based on XML using web services
  - XML (Extensible Markup Language): a meta-language that allows users to define their own customized way to describe data; the language used in CORE Connectivity to create CORE specific metadata
- Web Services Description Language (WSDL) is a document written in XML to describe a Web service (the software system to support machine-to-machine interactions over a network)
- Note: HTTP+MIME is not required in Phase IV CAQH CORE Connectivity Rule v4.0.0

Envelope Standard SOAP + WSDL
Real Time Request Message Structure (Non-normative–Instructional)

HTTP Headers

CORE Metadata in Use for SOAP 1.2 Request

The portion of the SOAP envelope in green has the metadata defined as part of the Phase IV CAQH CORE Connectivity Rule. (See §4.4)

The Real Time Payload file is in orange (MTOM attachment)

```
POST /CORE/PriorAuthRealTime HTTP/1.1
Host: server_host:server_port
Content-Type: multipart/related; boundary= MIMEBoundaryurn uuid 5117AAE1116EA8B87A1200060184614;
type="application/xop+xml"; start="0.urn:uuid:5117AAE1116EA8B87A1200060184615"; start-
info="application/soap+xml";
action="http://www.caqh.org/SOAP/WSDL/CORETransactions/RealTimeTransaction”

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:5117AAE1116EA8B87A1200060184615>

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
        <soapenv:Body>
              <ns1:COREEnvelopeRealTimeRequest
              xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule4.0.0.xsd">
                <PayloadType>X12_278_Request_005010X217E1_2</PayloadType>
                        <ProcessingMode>RealTime</ProcessingMode>
                        <PayloadID>f81d4fae-7dec-11d0-a765-00a0c91e6bf6</PayloadID>
                        <TimeStamp>2007-08-30T10:20:34Z</TimeStamp>
                        <SenderID>HospitalA</SenderID>
                        <ReceiverID>PayerB</ReceiverID>
                        <CORERuleVersion>4.0.0</CORERuleVersion>
                        <Payload>
                          <xop:Include href="cid:1.urn:uuid:5117AAE1116EA8B87A1200060184692"
                      xmlns:xop="http://www.w3.org/2004/08/xop/include" />
                        </Payload>
              </ns1:COREEnvelopeRealTimeRequest>
                </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614
Content-Type: image/jpeg
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:5117AAE1116EA8B87A1200060184692>

<Real Time Request Payload (e.g., a payload of type X12_278_Request_005010X217E1_2) goes here>

--MIMEBoundaryurn_uuid_5117AAE1116EA8B87A1200060184614--
```


CAQH CORE

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Security

The security aspects of the Rule are intended to assure:

- A message is not altered traveling between trading partner systems
- The message came from a known trading partner

Description of CAQH CORE Connectivity Rules
Connectivity Example with no intermediaries

Messages are protected while traveling to a destination

Submitter (Client)

Client and server must be known to each other in order to send requests

Health Plan (Server)

Note: CAQH CORE Connectivity Rules are a floor, not a ceiling

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Security Improvements

Stronger Submitter Authentication : X.509 Certificate over SSL/TLS
(Username and Password based authentication is not supported in Phase IV)

Entities requiring FIPS 140-2 compliance, or requiring higher transport security can use TLS 1.1 or higher in lieu of SSLv3, and SHA-2 (in lieu of SHA-1) for payload integrity using a checksum

Submitter (Client)

Federal Health Plan (Server)

Commercial Health Plan (Server)

TLS 1.1 or higher can be used for higher transport security but SSLv3.0 is also permitted

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Processing Modes for Transactions

Processing Mode:

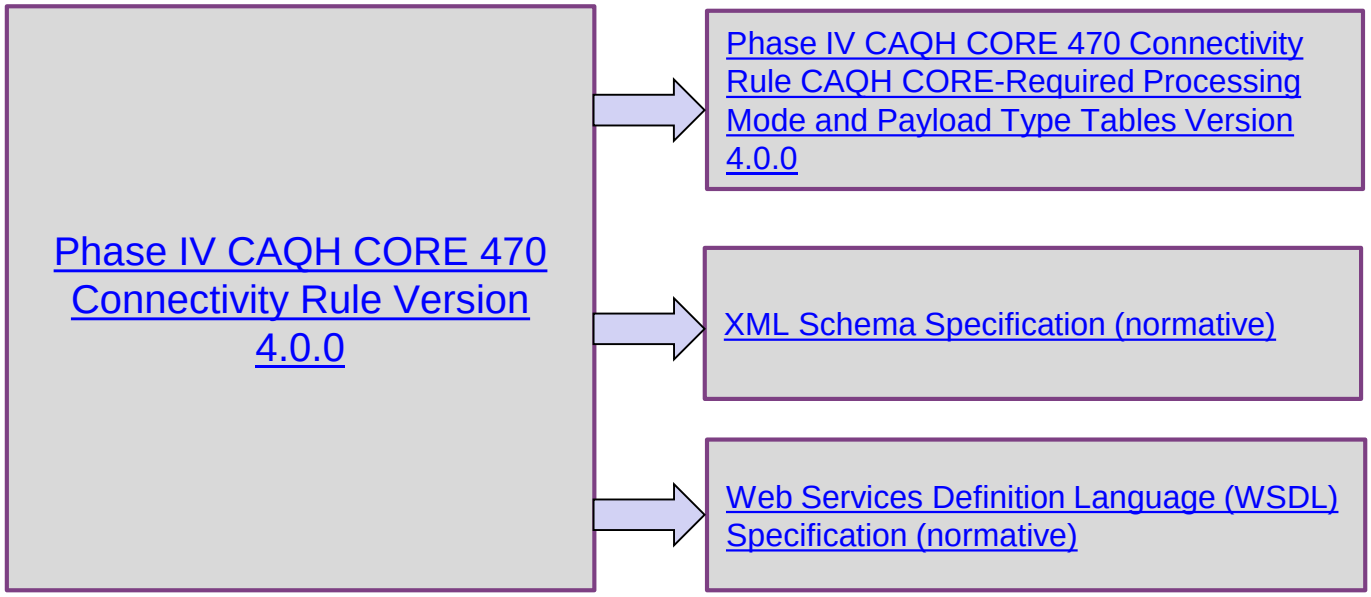
- Refers to how the payload of the connectivity message envelope is processed by the receiving system, in Real Time or Batch mode

Transaction	Processing Modes
ASC X12N 837 Version 5010 Health Care Claim (Institutional, Professional, Dental)	• Batch Mode Required • Real Time Mode Optional
ASC X12N Version 5010 278 Health Care Services Review – Request for Review and Response	Either Real Time Mode or Batch Mode Must be implemented • Both modes may be implemented
ASC X12N Version 5010 820 Payroll Deducted and Other Group Premium Payment for Insurance Products	• Batch Mode Required • Real Time Mode Optional
ASC X12N Version 5010 834 Benefit Enrollment and Maintenance	• Batch Mode Required • Real Time Mode Optional

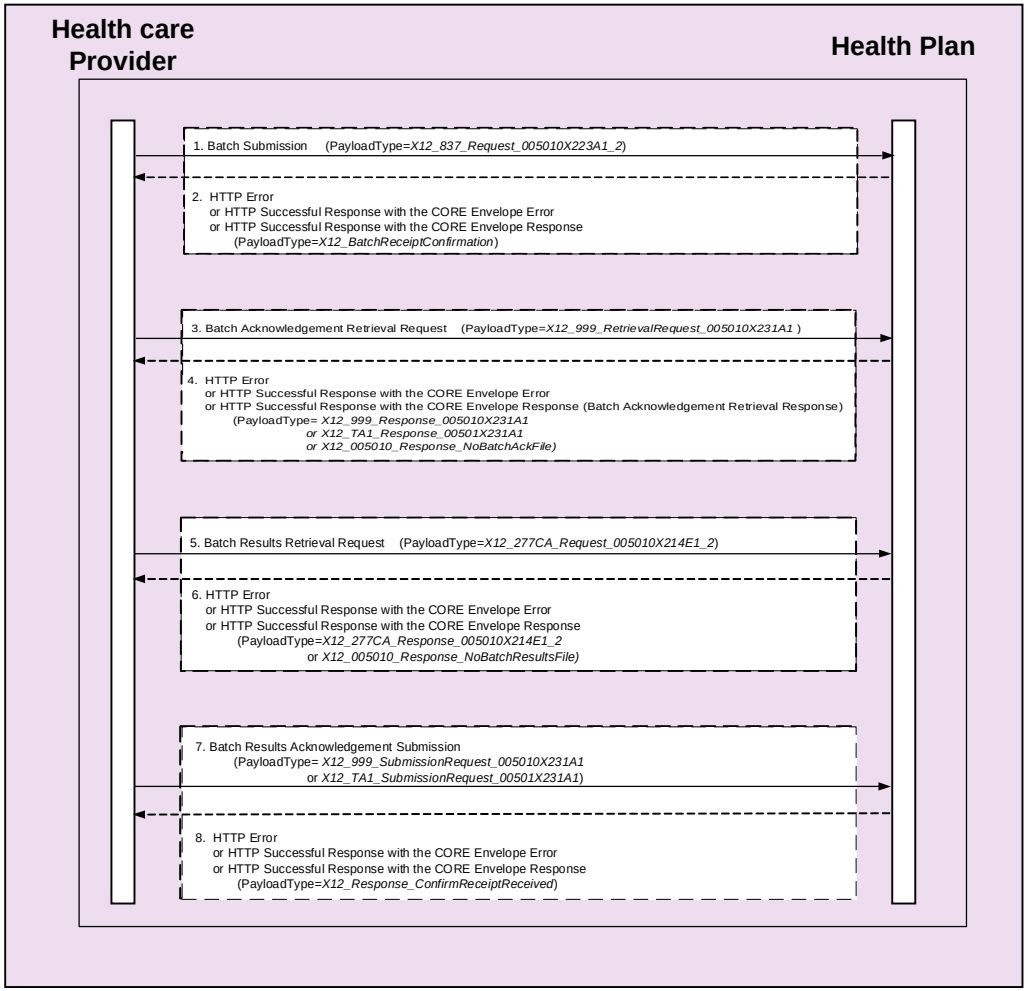
Note: The processing modes for the transactions are specified in a separate external document:
Phase IV CAQH CORE 470 Connectivity Rule CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0 §2 Processing Mode Table

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
External Documents

Resources

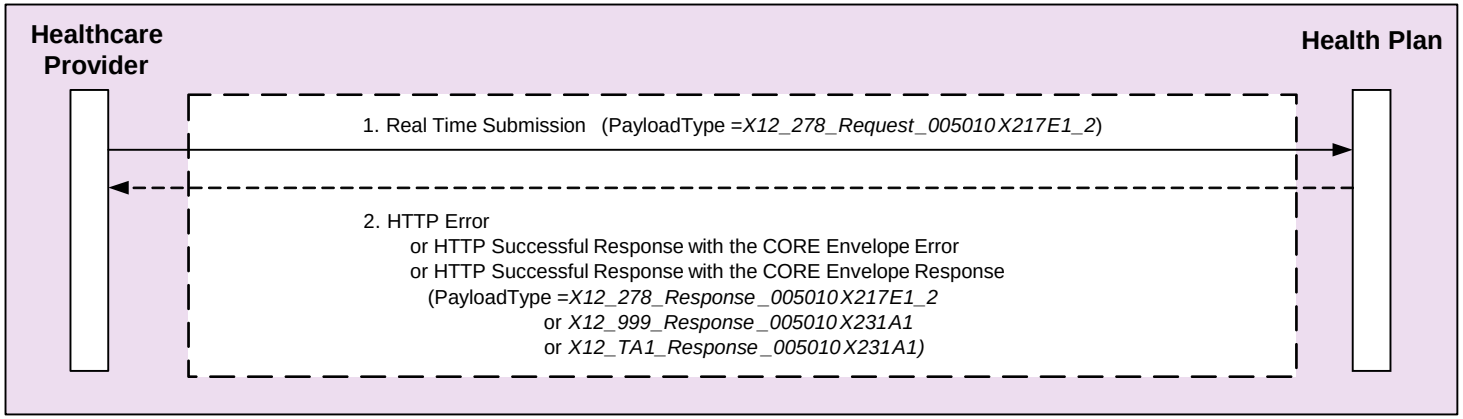


Message Interactions
Batch Claims (ASC X12 v5010 837) Batch Processing Mode Example



Message Interactions
Real Time Prior Authorization (ASC X12 v5010 278) Real Time Processing Mode Example

The payload for a Real Time message interaction consists of a single ASC X12 transaction



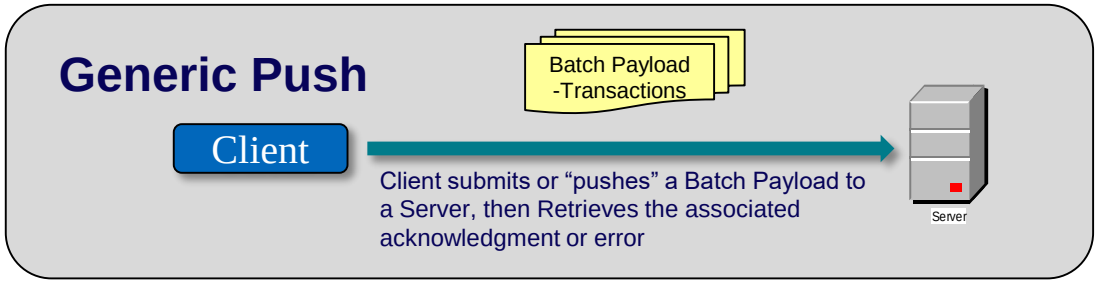
Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Enhancements to Message Interactions: Generic "Push" and "Pull" Models

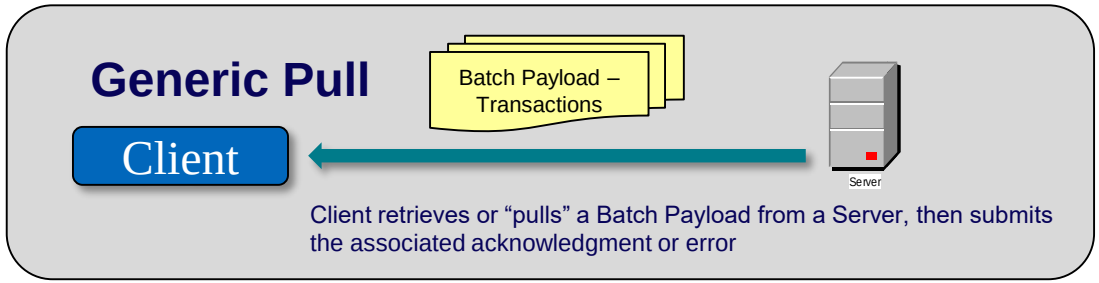
The Generic Push and Generic pull message interactions

- The Phase II CAQH CORE Connectivity Rule defined message interactions for conducting Real Time and Batch interactions
- Phase IV CAQH CORE Connectivity Rule keeps the Real Time and Batch interactions and added message interactions that could be used as generic building blocks for supporting current and future transactions
- The Generic Push and Pull Batch Interaction requirements support the conduct of the ASC X12N v5010 834 and the ASC X12N 5010 820 transactions

Benefits:

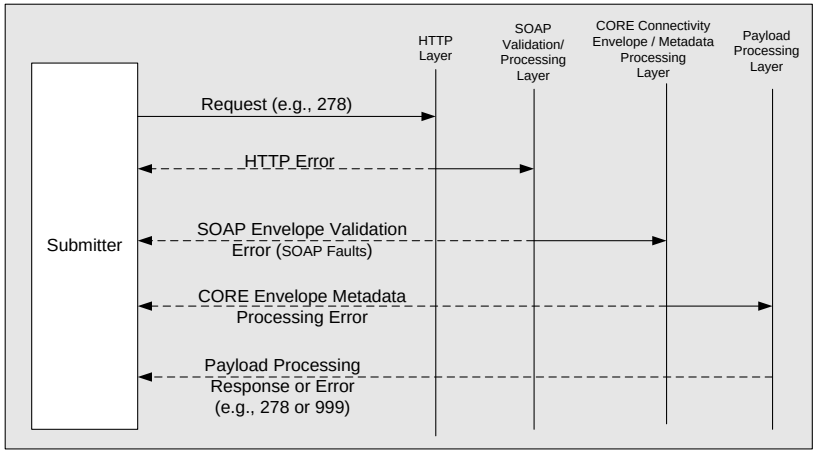
- Provides flexibility to support common industry message interactions for the ASC X12N v5010 820 and ASC X12N v5010 834 where:
  - A Health Plan Sponsor (Client), can "Push" a Batch to a Health Plan (Server)
  - A Health Plan (Client) can "Pull" a Batch from a Health Plan Sponsor (Server)





Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Error Handling Enhancements

- Error Handling occurs at HTTP, SOAP, CORE Envelope Metadata, and Payload Processing Layers
- CORE Connectivity Rules provides normative error codes and definitions for CORE Envelope Metadata processing
  - ✓ Error handling at HTTP, SOAP and Payload Processing Layers are not defined by CORE
- Phase IV CAQH CORE Connectivity Rule builds on error handling of Phase II CAQH CORE Connectivity Rule:
  - ✓ Addition of error codes based on implementer feedback
  - ✓ Removal of error codes that were required for HTTP+MIME based envelope metadata processing
  - ✓ Added examples and clarified the presentation of the error handling



Error Codes Added	Error description in Rule 470	Reason for Addition
<FieldName>UnSupported	Value is a legal value, but is not supported by the end point receiving the request. Server Connectivity Guide should indicate where to find specific SOAP Operations if multiple URLs are used to support Phase IV CAQH CORE Connectivity.	Implementer feedback from previous phases
NotSupported	A request was received at this server with a valid *PayloadType* or *ProcessingMode* but is currently not implemented by this server (e.g., it may be implemented at a different server within this organization)	Implementer feedback from previous phases

Error Codes Removed	Error description in Rule 270	Reason for Removal in Rule 470
<FieldName>Required	The field <FieldName> is required but was not provided	This is handled by SOAP Fault. Since Rule 470 does not have HTTP+MIME envelope, this error code is longer needed
<FieldName>NotUnderstood	The field <FieldName> is not understood at the receiver.	Same reason as above

Polling Question #2: Additional Education

What CAQH CORE Connectivity topics would you like to learn more about in future CAQH CORE educational webinars?

(Check all that apply)

1. CORE Safe Harbor Principle
2. CORE Connectivity Methods, i.e. SOAP, WSDL
3. Authentication Methods, i.e. digital certificates
4. Batch/Real Time Interaction Models

Resources and Additional Information

Robert Bowman
CAQH CORE Senior Manager

Phase IV CAQH CORE Analysis & Planning Guide Assists in Understanding Applicability of Rules to Various Trading Partners

*As with previous Phases, CAQH CORE now has an **Analysis & Planning Guide** for the Phase IV CAQH CORE Operating Rules*

Planning Guide should be used by project staff to:

Understand applicability of the Phase IV CAQH CORE Operating Rule requirements to organization's systems and processes that conduct the transactions

Identify all impacted external and internal systems and outsourced vendors that process the transactions

Conduct detailed rule requirements gap analysis to identify system(s) that may require remediation and business processes which may be impacted

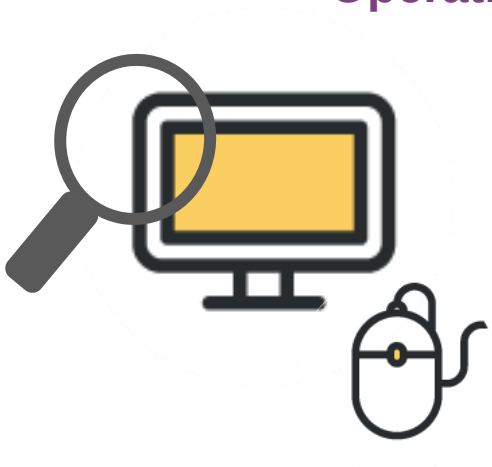
Planning Guides includes three tools to assist entities in completing analysis and planning:

1. Stakeholder & Business Type Evaluation
2. Systems Inventory & Impact Assessment Worksheet
3. Gap Analysis Worksheet

Phase IV CAQH CORE Operating Rules Frequently Asked Questions (FAQ)

New CAQH CORE FAQ Website

Includes more than 100 Phase IV FAQs addressing five Operating Rules and general concepts/questions



Newly revamped CAQH CORE FAQ website with *searchable*, web-based FAQs

(No more PDFs!)

New FAQ format will:

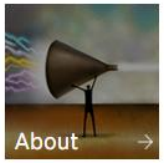
- **Enable users to more quickly find answers to their questions**
- **Allow users to search only the CAQH CORE FAQs for keywords**
- **View in one place all FAQs available for a given Operating Rule**

CAQH CORE

New CAQH CORE FAQ Website

CAQH

EVENTS NEWS CONTACT



Frequently Asked Questions

SEARCH CAQH CORE FAQS

FAQs

Join CORE

CAQH CORE PARTICIPANT CALENDAR

User ID (case sensitive)

Drew

Password (case sensitive)

•••••••

Login

four phases of the CAQH CORE Operating Rules, general CAQH CORE information, CORE Certification and future development of operating rules. You may find your FAQ by clicking on the links below or using the search bar above to identify key words.

Additional CAQH CORE Resources are available for implementing the CAQH CORE Operating Rules: See CAQH CORE Implementation Resources and CAQH CORE Events.

If you have any questions not addressed by the CAQH CORE Online Resources, please email CORE@caqh.org.

NOTE: The CAQH CORE FAQs are for informational purposes only; in the case of a discrepancy between this document and CAQH CORE Operating Rule text and/or Federal regulations, the latter take(s) precedence. No adjustments to CAQH CORE rule requirements will be made via the FAQ process.

- PART A: GENERAL CAQH CORE FAQS
- PART B: ACA SECTION 1104 MANDATE FOR FEDERAL OPERATING RULES
- PART C: PHASE I & II CAQH CORE ELIGIBILITY & CLAIM STATUS OPERATING RULES
- PART D: PHASE III CAQH CORE EFT & ERA OPERATING RULES
- PART E: PHASE IV CAQH CORE OPERATING RULES
- PART F: CAQH CORE OPERATING RULES IN DEVELOPMENT
- PART G: CERTIFICATION: ACA SECTION 1104 CERTIFICATION, CORE CERTIFICATION, PROPOSED CORE HIPAA CREDENTIAL, AND CORE ENDORSEMENT

PART A: GENERAL CAQH CORE FAQS

General FAQs address CAQH CORE's background and mission, the CAQH CORE Rules Development Process, and procedures and policies related to CORE Participation, CORE Certification, and CORE Endorsement.

I. Overview of CAQH CORE

General CAQH CORE FAQs

I. Overview of CAQH CORE

List Order

1. What is CAQH CORE?
2. What is CAQH?
3. What are operating rules?
4. Why develop operating rules for exchange of healthcare administrative information?
5. What are the CAQH CORE Guiding Principles and where can they be located?
6. Will CAQH CORE build a database?
7. How do the CAQH CORE Operating Rules work?
8. How were the CAQH CORE Operating Rules created?
9. How will the CAQH CORE Rules be updated?

1. What is CAQH CORE?

The Committee on Operating Rules for Information Exchange (CORE) is a multi-stakeholder initiative of CAQH. CAQH CORE was established in 2005 with the mission to build consensus among healthcare industry stakeholders on a set of operating rules that facilitate administrative interoperability between providers and health plans.

Since its inception, CAQH CORE has been structured around a model that operating rules authoring entities should take the responsibility of going above and beyond authorship to help drive adoption. To do this, CAQH CORE applies an integrated model in which CAQH CORE:

- Develops operating rules through broad-based stakeholder input that supports using standards.
- Develops and offers a certification program that ensures operating rules are objectively and rigorously tested and, thus, there is a solid base of early implementers.
- Builds broad-based awareness of the operating rules.
- Provides in-depth, detailed technical knowledge and assistance through early adopters.
- Promotes operating rules adoption by a majority of all stakeholders

CAQH CORE

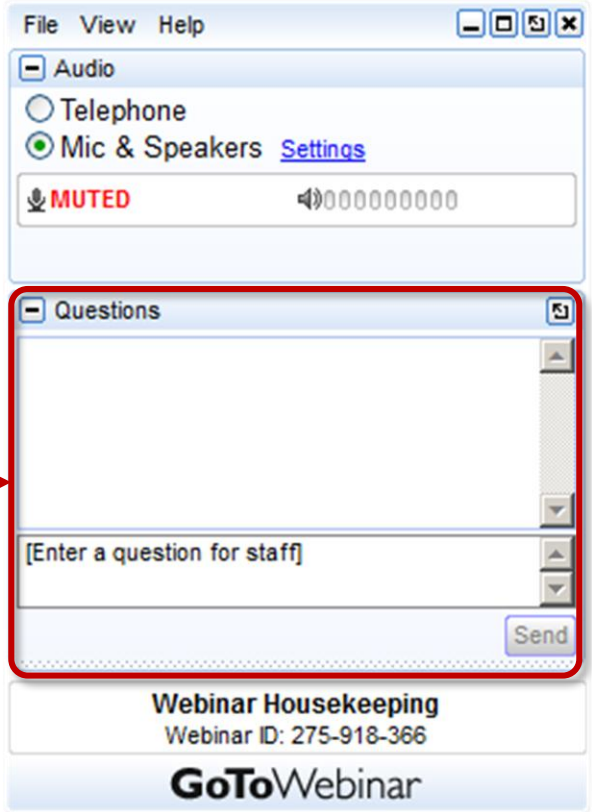
CAQH CORE Connectivity Rules
Frequently Asked Questions - Examples

Questions	
Basic Conformance Requirements for Key Stakeholders (Rule Section 4) I am a Healthcare Provider. Do I need to support a Client or Server roles or both for exchanging the HIPAA-mandated transactions?	The Phase IV CAQH CORE Operating Rules define minimum technical roles for a HIPAA-covered health plan or its agent. The CAQH CORE 470 Rule defines message interactions between providers and health plans which require that at a minimum a provider support a Client role as described in the CAQH CORE 470 Rule for exchanging the HIPAA-mandated transactions addressed in the Phase IV CAQH CORE Operating Rules.
Submitter Authentication / X.509 certificate authentication (Rule Section 4.1.2) Does the Phase IV CAQH CORE 470 Connectivity Rule have any requirements for the digital certificates used for authentication; e.g., an acceptable Certificate Authority, Certificate Version, Key Length, Public Key Expiration Date, etc.?	No. The CAQH CORE 470 Rule does not specify any security requirements for administering and managing the X.509 Digital Client Certificate. Section 4.3, *Publication of Entity-Specific Connectivity Companion Document*, of the Rule recommends that server organizations specify their X.509 Digital Certificate requirements in their Connectivity Companion Document.
SOAP+WSDL Envelope Standard (normative) (Rule Section 4.1.3) Why are non-normative descriptions provided?	Non-normative descriptions are informational and educational descriptions only on the use of the normative SOAP+WSDL envelope specifications, and are not intended to be part of the specification.

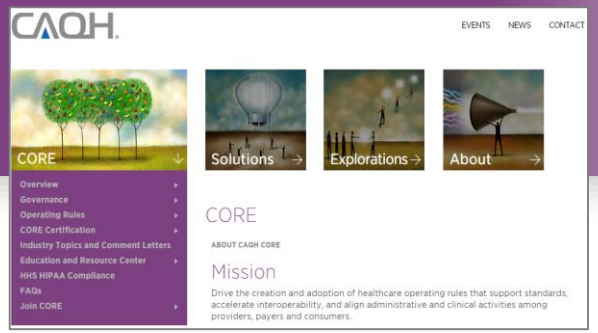
Audience Q & A

Please submit your questions

Enter your question into the “Questions” pane in the lower right hand corner of your screen.



Engage with CAQH CORE!



CAQH CORE Website

or contact us at CORE@CAQH.org

Participate in the CAQH CORE Code Combinations Task Group (CCTG) or the Enrollment Data Task Group

Become a CAQH CORE Participating Organization

Explore Voluntary CORE Certification

Register for our educational webinars

Dedicated webpages:

- ✓ Code Combination Maintenance
- ✓ EFT/ERA Enrollment Maintenance
- ✓ Voluntary CORE Certification
- ✓ CAQH CORE Phase IV Operating Rules

CAQH CORE

Thank you for joining us!

Website: www.CAQH.org/CORE

Email: CORE@CAQH.org

@CAQH

CAQH CORE

Appendix

Final versions of each rule are available for free on our website (www.CAQH.org/CORE):

Phase IV CAQH CORE 450 Health Care Claim (837) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 452 Health Care Services Review – Request for Review and Response (278) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 454 Benefit Enrollment & Maintenance (834) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 456 Premium Payment (820) Infrastructure Rule Version 4.0.0

Phase IV CAQH CORE 470 Connectivity Rule Version 4.0.0

- XML Schema Specification (normative)
- Web Services Definition Language (WSDL) Specification (normative)
- Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables Version 4.0.0

Server Requirements

Server: An entity that receives a message from a Client, which it may process, or relay to another Server

- Ability to receive incoming connections over the public Internet
- Ability to authenticate the incoming connections using the X.509 Client Digital certificate based authentication over SSL Version 3 or TLS 1.1 or higher
- Ability to parse and process the message envelope using the SOAP+WSDL standard as specified in the v4.0.0 XSD and WSDL
- Ability to process the 3rd set of ACA mandated transactions with the processing modes as specified in the Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables v4.0.0
- Ability to receive the payload types specified in the Phase IV CAQH CORE-Required Processing Mode and Payload Type Tables Version 4.0.0 and process the payload types
- Perform error processing
- Track the date, time and payload ID of messages
- Meet the Availability and Response time requirements specified in the CAQH CORE Phase IV Infrastructure Rules
- Publish an Entity-Specific Connectivity Companion Document

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
Security Across the Layers - Improved Support for Security and Compliance

Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over a common medium

- Security requirements:
  - Secure Socket Layer (SSL) Version 3.0 is a standard security technology for establishing an encrypted link between two servers
    - Provides "over the wire" (or transport level) confidentiality and integrity of the data sent over the SSL/TLS session
    - Servers are authenticated using SSL Server Certificates
    - Requires SSL Version 3.0 or optionally TLS 1.1 or higher for transport level security
      - Entities that must also be FIPS 140-2 compliant or whose security policies require enhanced security may implement TLS 1.1 or higher in lieu of SSL Version 3.0.
  - For authenticating clients (i.e., "Submitters"):
    - X.509 Certificates over SSL (optionally TLS 1.1 or higher)
  - For payload integrity verification:
    - SHA-1 A Checksum of the payload is sent as part of the message envelope.
      - Entities requiring FIPS 140-2 compliance may use SHA-2 instead of SHA-1.
      - If SHA-2 is used, then the entity's Connectivity Companion Document can specify that SHA-2 is expected in incoming messages from trading partners.
  - For reliability of transport:
    - UUID* is used for Payload ID (for detecting duplicates)
    - Timestamp is used for ensuring that the data is recent

Related Trends:

- SSL Version 3.0 is commonly used in the industry
- TLS 1.1 or higher is used for securing connections with Federal government trading partners
- HealtheWay - eHealth Exchange (formerly NwHIN Exchange) (included in Meaningful Use-2) uses TLS
- ONC S&I Electronic Submission of Medical Documents (esMD) and Electronic Determination of Coverage (eDoc) use TLS

Phase IV CAQH CORE 470 Connectivity Rule v4.0.0
X.509 Digital Certificate: A Single Submitter Authentication Method

Submitter Authentication

- **X.509 digital certificate** as the single authentication standard
  - Username + password was removed

Benefits:

- X.509 Client Certificate based authentication over SSL/TLS is stronger than username + password
- Reduced implementation cost and complexity having one standard
- Client certificate based authentication requires the submitter to access its cryptographic key (private key) to use its public key certificate
- Digital Certificates
  - expire and need to be renewed, the potential for a successful brute force attack is low
  - can be revoked through a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) mechanism
- Aligned with clinical initiatives and industry trends (e.g., NwHIN Exchange) that use SOAP over HTTP for clinical data exchanges, and use client certificate based authentication for Business-to Business authentication

Background:

The CAQH CORE Connectivity Rule Version 2.2.0 has two submitter authentication standards:

- X.509 Client Authentication over SSL Version 3.0 or TLS 1.0 (FIPS 140)
- Username-Password

Scope

ASC X12 Transactions Addressed by the Phase IV CAQH CORE Connectivity Rule, Relationship to Previous Phases

Phase I & II	Phase III	Phase IV
• ASC X12 005010X279A1 Eligibility Benefit Request and Response (270/271) • ASC X12 005010X212 Health Care Claim Status Request and Response (276/277)	• ASC X12 005010X221A1 Health Care Claim Payment/Advice (835) Note: the CAQH CORE Connectivity Rules *do not apply* to the Health Care Electronic Funds Transfers transaction	• ASC X12N 005010X223 Health Care Claim Institutional (837) • ASC X12N 005010X222 Health Care Claim Professional (837) • ASC X12N 005010X224 Health Care Claim Dental (837) *(collectively referred to as ASC X12N 837 v5010 Claim)*
		ASC X12N 005010X217 Health Care Services Review – Request for Review and Response (278) *(generally referred to as Prior Authorization)*
		ASC X12N 005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820) *(generally referred to as Health Plan Premium Payment)*
		ASC X12N 005010X220 Benefit Enrollment and Maintenance (834) *(generally referred to as Benefit Enrollment)*
		Note: *Although the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 addresses the transactions above all transactions addressed by all phases of CAQH CORE Operating Rules can be conducted under the Safe Harbor provisions of the either the Phase IV CAQH CORE 470 Connectivity Rule v4.0.0 or the HIPAA-mandated Phase II CAQH CORE 270 Connectivity Rule v2.2.0. Entities must still implement the HIPAA-mandated Phase II CAQH CORE Phase II Connectivity Rule v2.2.0.*

Note: References to ASC X12 transactions also include all associated errata

Technical Requirements and the Relationship to the Phase I-III Requirements

Connectivity Rule Area	CORE Phase I Connectivity Rule Requirements	CORE Phase II & III Connectivity Rule Requirements	CORE Phase IV Connectivity Rule Requirements
Network	Internet	Internet	Internet
Transport	HTTP	HTTP	HTTP
Transport Security	SSL	SSL 3.0 with optional use of TLS 1.x	SSL 3.0, or optionally TLS 1.1 or higher. • Entities that must also be FIPS 140-2 compliant or that require stronger transport security may implement TLS 1.1 or higher in lieu of SSL 3.0
Submitter (Originating System or Client) Authentication	Name/Password	• UserName + Password or • X.509 Digital Certificate	X.509 Digital Certificate based authentication over SSL/TLS • *Removed Username + Password*
Envelope and Attachment Standards	Unspecified	SOAP 1.2 + WSDL 1.1 and MTOM (for Batch) or HTTP+MIME	SOAP 1.2 + WSDL 1.1 and MTOM (for both Real Time and Batch) • *Removed HTTP+MIME*
Envelope Metadata	Unspecified	Metadata defined (Field names, values) (e.g., *PayloadType, Processing Mode, Sender ID, Receiver ID*)	• Metadata defined (Field names, values) (e.g., *PayloadType, Processing Mode, Sender ID, Receiver ID*) • SHA-1 for Checksum • FIPS 140-2 compliant implementations can use SHA-2 for checksum.
Message Interactions/ Routing	• Real-time • Batch (Optional if used)	• Real-time • Batch (Optional if used)	• Batch and Real-Time processing requirements defined for each transaction • Push and Pull Generic messages for 820/834 transactions
Acknowledgements, Errors	Specified	Enhanced Phase I, with additional specificity on error codes	Errors Codes updated
Basic Conformance Requirements for Client and Server Roles	Minimally specified	Well specified	Well specified
Response Time	Specified	Maintained Phase I time requirements	Maintained Phase I time requirements
Connectivity Companion Guide	Specified	Enhanced Phase I, with additional recommendations	Enhanced Phase I, with additional recommendations

CAQH CORE