Committee on Operating Rules For Information Exchange (CORE®)

Got SOAP? Educating IT on the Federally Mandated CAQH CORE Connectivity Operating Rules

June 19, 2012

Erin Richter
CORE Senior Manager
CAQH

Raja Kailar
Chief Technology Officer
Kevin Castellow
Consultant
Business Networks International, Inc.

David Querusio
Director, eBusiness Architecture
Harvard Pilgrim Health Care, Inc.

Session Learning Objectives

Attendees will:

- Understand the principles and technical concepts that form the basis for the mandated CAQH CORE Connectivity Rules including alignment with other Federal HIT initiatives
- Learn the detailed requirements of the mandated CAQH CORE Connectivity Rules for the eligibility and claim status transactions
- Be prepared to conduct informed internal analysis and planning for implementation of the mandated CAQH CORE Connectivity Rules

simplifying healthcare administration
CAQH

Snapshot of Call Participants

- More than 350 individuals representing more than 175 unique entities (both CORE and non-CORE Participating Organizations)
  - All key stakeholder groups including:
    - Health Plans
    - Providers
    - Vendors
    - Clearinghouses
    - Government Entities
    - Associations
  - Range of technical and non-technical experts, examples of titles include:
    - EDI Director
    - Solutions Architect
    - IT Manager
    - Developer
    - Project Manager
    - Business Analyst/Consultant
    - Compliance Analyst
    - Product Manager

simplifying healthcare administration
CAQH®

Agenda

Topic	Time
Level-Set: CAQH CORE & ACA Section 1104	5 minutes
Mandated CAQH CORE Connectivity Rules*: Enhancing the Industry Landscape	5 minutes
Mandated CAQH CORE Connectivity Rules: Key Technical Concepts Addressed	15 minutes *(Includes Q&A on Technical Concepts)*
Mandated CAQH CORE Connectivity Rules: Detailed Rule Requirements	30 minutes *(Includes Q&A on Rule Requirements)*
Implementing the Mandated CAQH CORE Connectivity Rules: Perspectives from a CORE-certified Health Plan	10 minutes
Implementing the Mandated CAQH CORE Connectivity Rules: Additional Guidance	5 minutes
General Q & A and Session Evaluation	10 minutes
Appendix: CAQH CORE Resources for Implementing the CAQH CORE Connectivity Rules	

**For the purposes of this presentation, the Phase I & II CAQH CORE Connectivity Rules (Rules 153 & 270 respectively) are referred to jointly as the CAQH CORE Connectivity Rules.*

simplifying healthcare administration
CAQH

Level-Set: CAQH CORE & ACA Section 1104

simplifying healthcare administration
CAQH®

CAQH® and Its Initiatives

CAQH, a nonprofit alliance of health plans and trade associations, is a catalyst for industry collaboration on initiatives that simplify healthcare administration for health plans and providers, resulting in a better care experience for patients and caregivers.

CORE®
Committee on Operating Rules for Information Exchange

Multi-stakeholder collaboration of over 130 participating organizations that is developing industry-wide operating rules, built on existing standards, to streamline administrative transactions. Cover 75% of the commercially insured, plus Medicare and some Medicaid.

Universal Provider Datasource®

An industry utility that replaces multiple health plan paper processes for collecting provider data with a single, electronic, uniform data-collection system (i.e., credentialing). More than 1 million providers self-report their information to UPD and over 650 organizations access the system, including a range of public and private entities.

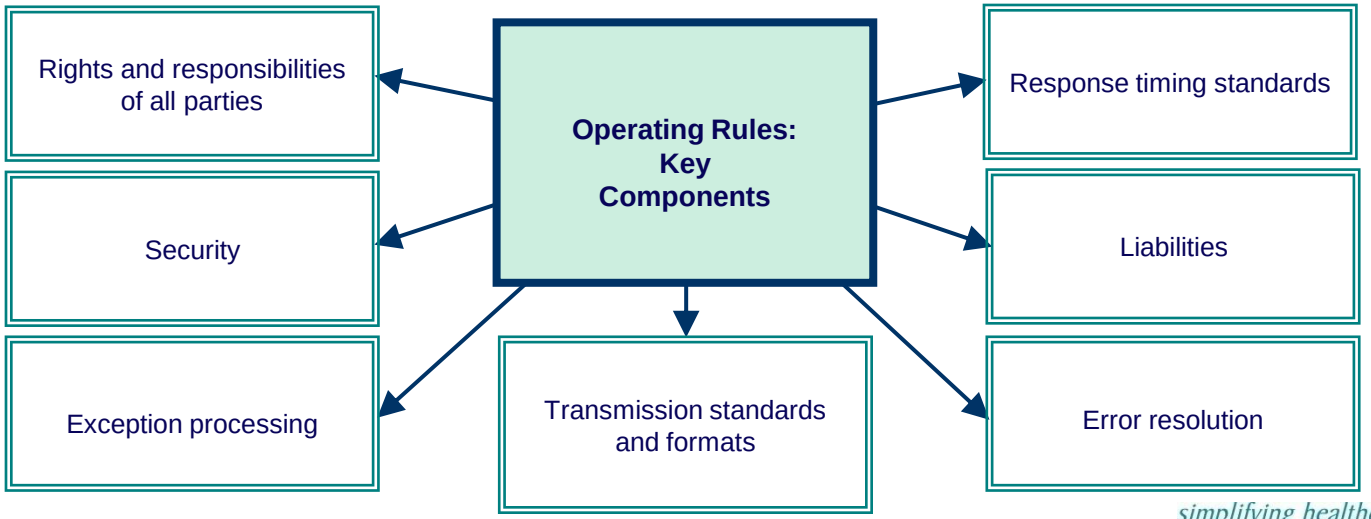
US HEALTHCARE® EFFICIENCY INDEX

An objective industry forum for monitoring business efficiency in healthcare. Tracking progress and savings associated with adopting electronic solutions for administrative transactions across the industry.

simplifying healthcare administration
CAQH®

What Are Operating Rules?

- The Patient Protection and Affordable Care Act (ACA) defines operating rules
  - Operating rules address gaps in standards, help refine the infrastructure that supports electronic data exchange, and recognize interdependencies among transactions; they do not duplicate standards
  - Current healthcare operating rules build upon a range of standards – healthcare specific (e.g., ASC X12) and industry neutral (e.g., OASIS, W3C, ACH CCD+) – and support the national HIT agenda
- Operating rules encourage an interoperable network and, thereby, are vendor agnostic



simplifying healthcare administration

CAQH

Overview: *ACA Section 1104*

- ACA Section 1104 requires Secretary of Health and Human Services (HHS) to adopt and regularly update operating rules for *three sets* of healthcare financial and administrative transactions
  - Operating rules address gaps in standards, help refine the infrastructure that supports electronic data exchange, and recognize interdependencies among transactions; *do not replicate the standards*
  - First set addresses Eligibility for a Health Plan and Health Care Claim Status transactions
    - December 2011: HHS adopted the CAQH CORE Eligibility & Claim Status Operating Rules to fulfill the Federal mandate, *with the exception of requirements for use of Acknowledgements and completion of voluntary CORE Certification*
    - HIPAA covered entities must meet all applicable technical requirements of the CAQH CORE Eligibility & Claim Status Operating Rules by the effective date of **January 1, 2013**
- For more information on ACA Section 1104, see the following resources:
  - CMS information on the ACA Administrative Simplification provisions including timelines for adoption, implementation, and compliance
  - CMS information on the ACA compliance, certification, penalties, and enforcement processes
  - CMS information on the HIPAA Administrative Simplification provisions
  - CAQH CORE overview of the Federal mandate for eligibility & claim status operating rules
  - Materials and recordings from past CAQH CORE Education Sessions
    - Additional CAQH CORE resources related to the Federally mandated eligibility & claim status operating rules are described in the Appendix

simplifying healthcare administration
CAQH

Mandated Eligibility & Claim Status Operating Rules: *Scope*

Topics that the CAQH CORE Eligibility & Claim Status Operating Rules Address: *All are within ACA-defined scope of operating rules and build on standards where appropriate*		
Data Content: ***Eligibility***	Address Need to Drive Further Industry Value in v5010 Investment	More Robust Eligibility Verification Plus Financials Enhanced Error Reporting and Patient Identification
Infrastructure: ***Eligibility and Claim Status***	Address Industry Needs for Common/ Accessible Documentation	Companion Guides System Availability
	Address Industry-wide Goals for Architecture/ Performance/ Connectivity	Response Times Acknowledgements* Connectivity and Security

***NOTE**: In the Final Rule for *Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction*, requirements pertaining to use of Acknowledgements are NOT included for adoption. Although HHS is not requiring compliance with any operating rule requirements related to Acknowledgements, the Final Rule does note "we are addressing the important role acknowledgements play in EDI by strongly encouraging the industry to implement the acknowledgement requirements in the CAQH CORE rules we are adopting herein."

simplifying healthcare administration CAQH

30-Second Poll:
Familiarity With the Federally Mandated CAQH CORE Connectivity Rules

simplifying healthcare administration
CAQH

Mandated CAQH CORE Connectivity Rules:

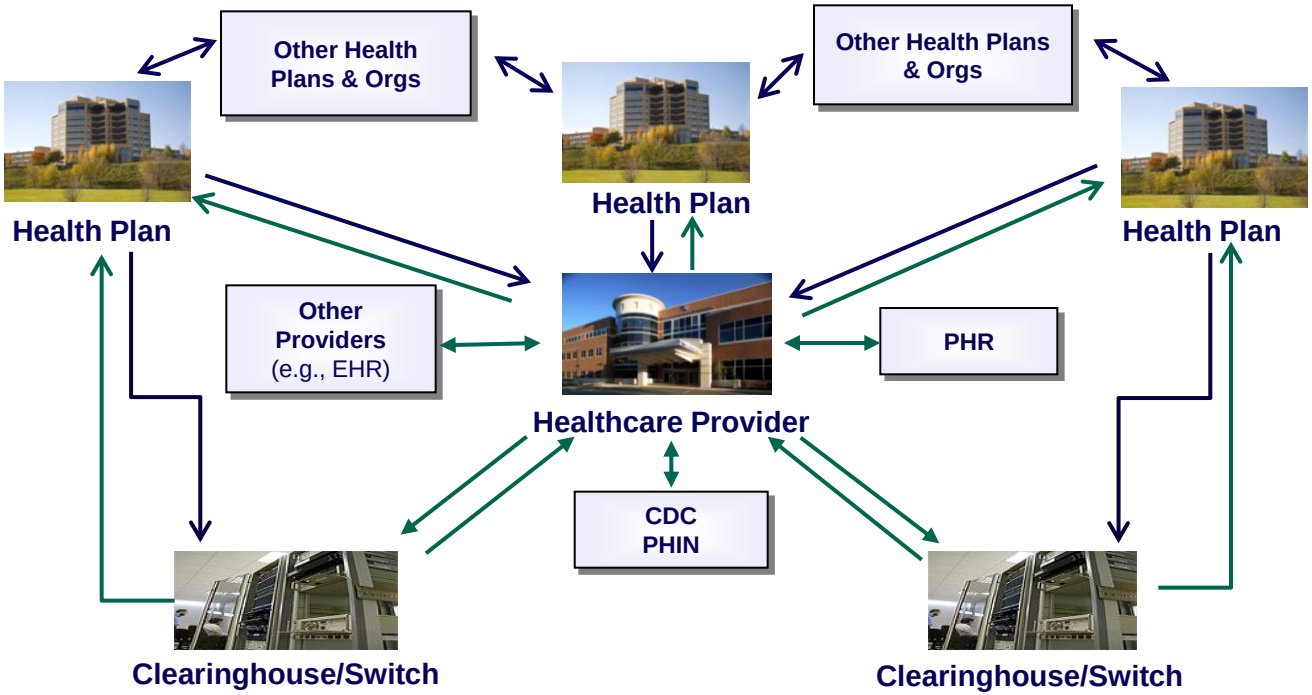
Enhancing the Industry Landscape

simplifying healthcare administration

CAQH®

CORE Connectivity: *Industry Landscape*

- Currently, multiple connectivity methods are utilized across the industry
  - Providers/health plans need to support multiple methods to connect to multiple health plans, clearinghouses, and other provider organizations



- CORE Connectivity Rules enhance interoperability and efficiency by defining technical requirements for trading partner exchange of administrative transactions
  - CORE Connectivity can be applied independent of the communication architecture or model

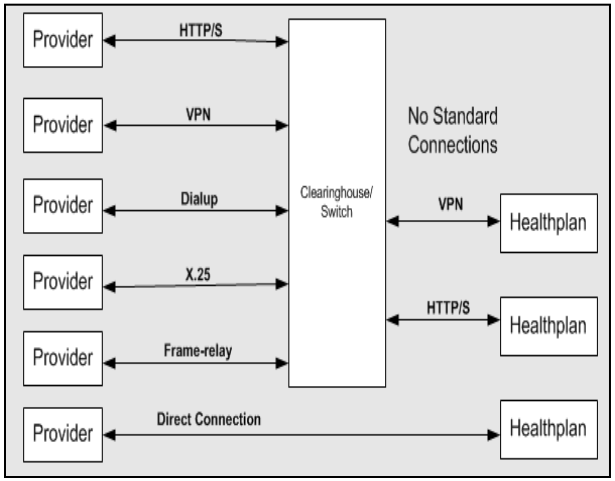
simplifying healthcare administration
CAQH

CORE Connectivity: *Moving the Industry Forward*

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

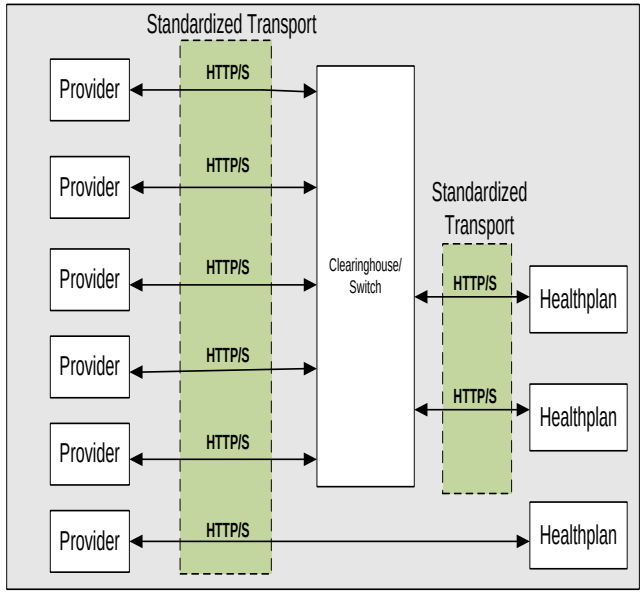
Increased interoperability & improved connectivity

Prior to CORE Connectivity: No Uniform Connection Standard



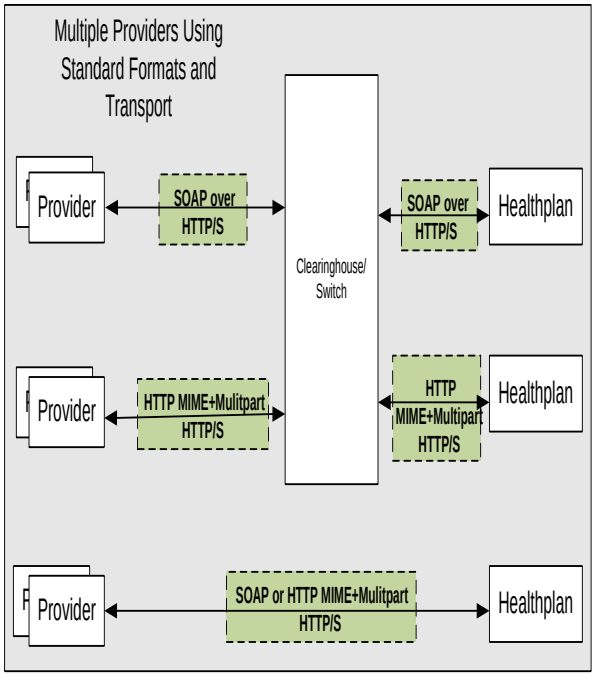
Costly management of multiple protocols, many proprietary

Phase I CORE Connectivity: Standardized Transport



Greater online access due to uniformity in transport protocols

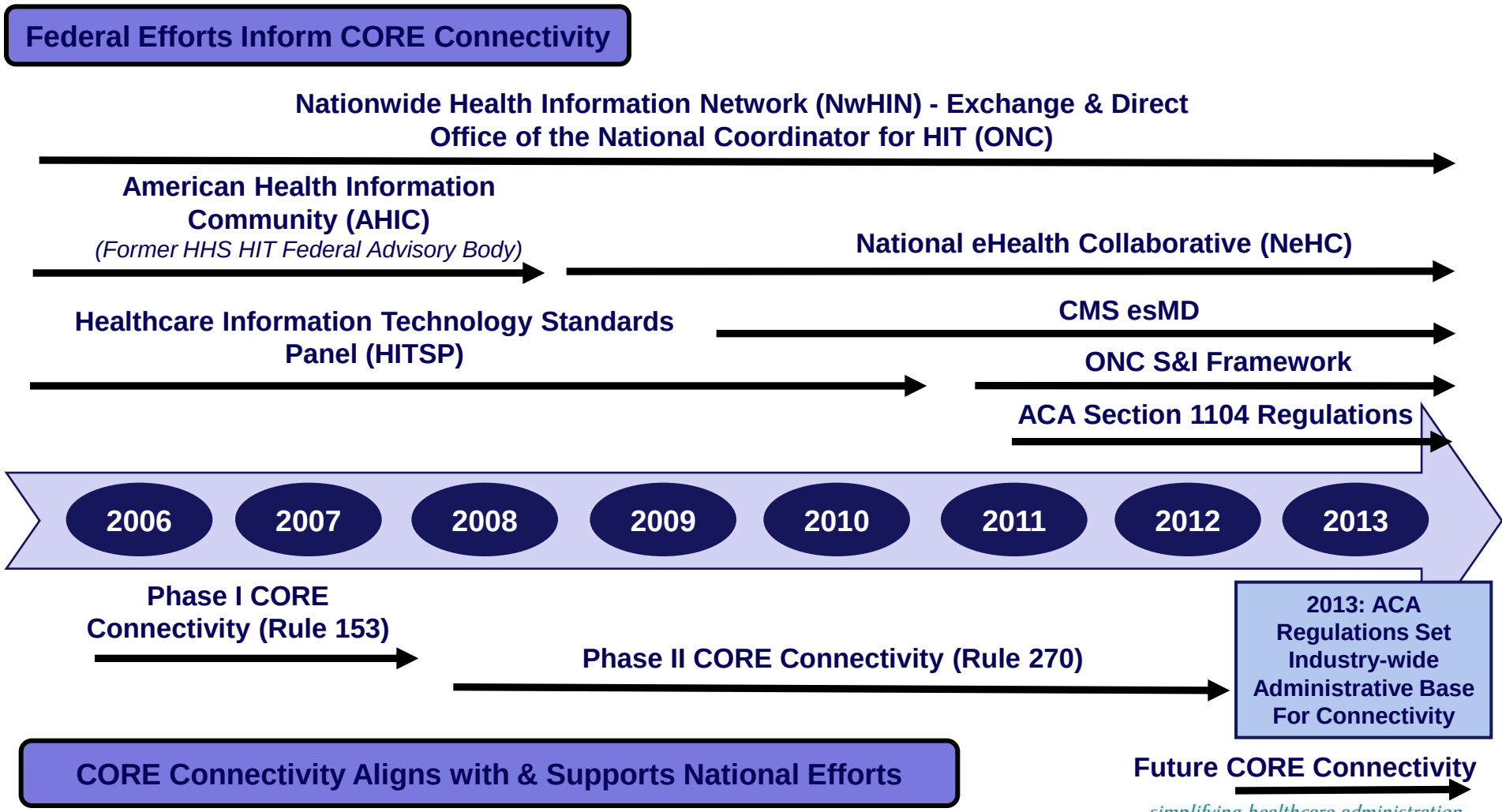
Phase II CORE Connectivity: Common Transport & Envelope Standards



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

CORE Connectivity: *Industry Alignment*

CORE Connectivity supports/integrates with other efforts to create alignment across the industry



simplifying healthcare administration

CAQH®

CORE Connectivity: *Alignment with Federal HIT Efforts*

- Alignment occurs by establishing common components and approaches across initiatives
  - Payoff of alignment with national initiatives is the potential to leverage cross-over of clinical and administrative transactions, as appropriate, and have informed expertise when determining next milestone
- Nationwide Health Information Network (NwHIN)
  - CAQH CORE has collaborated with NwHIN initiatives for many years to support alignment of standards for healthcare connectivity
  - CORE Connectivity Rules are designed to align with NwHIN; future rules will continue alignment
- CMS Electronic Submission of Medical Documentation (esMD) Program
  - CORE Connectivity Rule 270 is used to specify connectivity in the X12 Profile of CMS esMD Phase I
  - CAQH CORE is actively contributing to CMS esMD Phase II, now an ONC Standards & Interoperability (S&I) Framework Initiative
- CMS Medicaid Information Technology Architecture (MITA)
  - Emphasis on partnering with CMS in refining MITA to ensure alignment with the administrative simplification needs of Medicaid
- Close coordination with other key health IT efforts including ONC S&I Framework, HITSP, NeHC, etc.

simplifying healthcare administration
CAQH

30-Second Poll:
Status of Your Organization's CAQH CORE Connectivity Implementation

simplifying healthcare administration
CAQH

Mandated CAQH CORE Connectivity Rules:

Key Technical Concepts Addressed

simplifying healthcare administration

CAQH®

CORE Connectivity: *Technical Standards*

- CORE Connectivity Rules build on technical standards to define how messages are packaged and transmitted between trading partners
  - Specifications on Envelope Metadata and structure
  - Authentication standards
  - Defined Payload Types
  - Message interactions
  - Error handling
- CORE Connectivity Rules are based on the following standards:
  - HTTP Version 1.1
  - SSL Version 3.0
  - MIME Version 1.0
  - The MIME Multipart/Form-Data (IETF RFC 2388)
  - SOAP Version 1.2
  - WSDL Version 1.1
  - Web Services-Security 1.1

simplifying healthcare administration
CAQH®

CORE Connectivity: *Layered View*

- Open Systems Interconnection Basic Reference Model (OSI model) is a common conceptual framework describing a network communication system
  - *Each layer serves the layer above it*

Application (i.e., Business Processing) Layer (Layer 7):

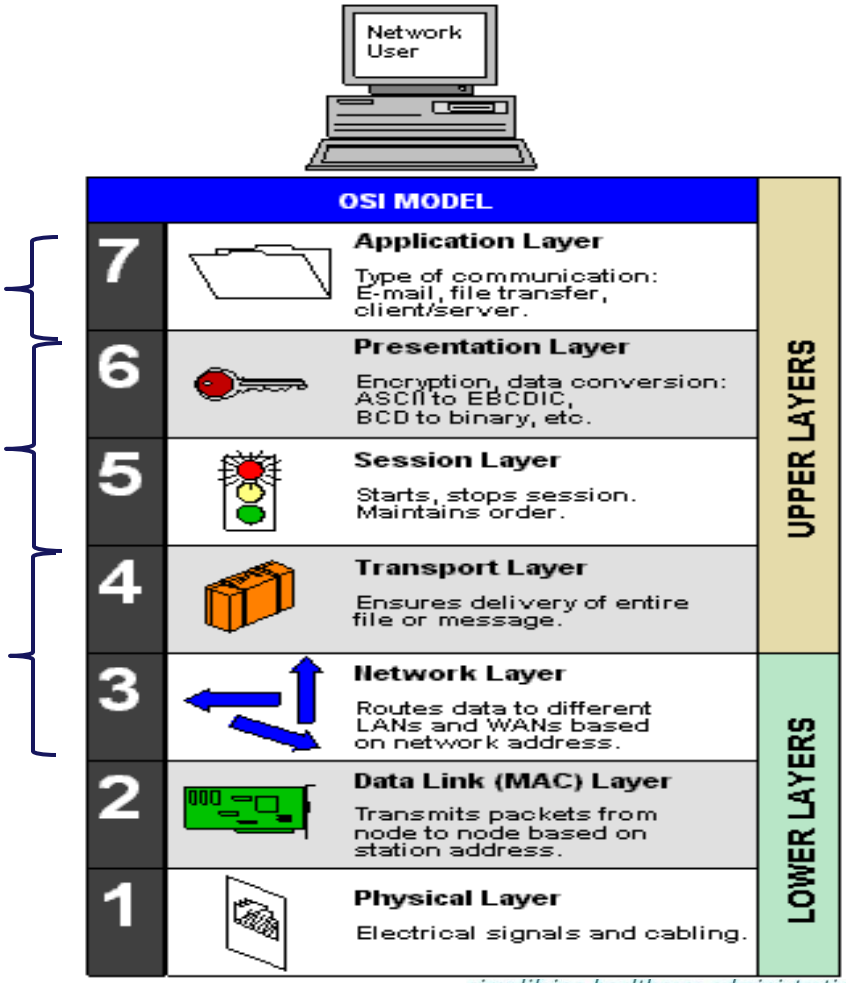
Application file (i.e., Payload) is created/processed by application

Message Encapsulation Layer (Layers 5 & 6):

Creates message envelope and handles connectivity/security

Message Transport Layer (Layers 3 & 4):

Provide necessary message transport and network infrastructure



simplifying healthcare administration

CAQH®

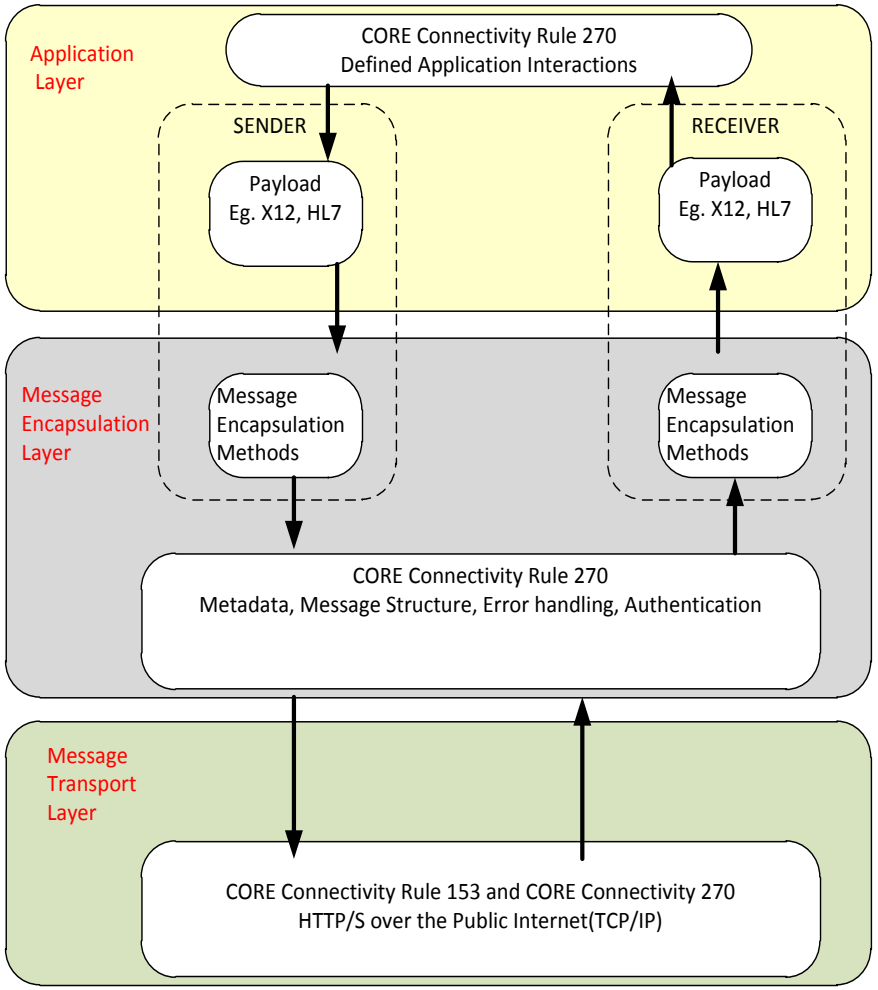
CORE Connectivity: *Layered View cont'd*

The OSI Model: Where The CORE Connectivity Rules Apply

- **Application (i.e., Business Processing) Layer:**
  - CORE Connectivity Rules are "Payload Agnostic", hence do not specify the Application file or processing layer

- **Message Encapsulation Layer:**
  - CORE Connectivity Rule 270 defines a prescriptive Message Envelope structure and metadata

- **Message Transport Layer:**
  - CORE Connectivity Rules prescribe use of a securely encrypted Message Transport Layer
    - Rules require HTTP over SSL; CORE Connectivity Rule 270 includes optional use of TLS

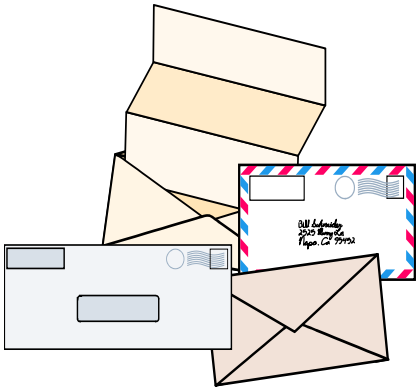


simplifying healthcare administration

CAQH®

Message Encapsulation Layer: *Envelopes & Metadata*

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



- 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)
  - In CORE Connectivity, Message Envelope consists of a well-defined structure for organizing and formatting Message Envelope Metadata
  - CORE Message Envelope Metadata help message receivers route messages for internal processing without opening envelope, reducing costs and improving response time
  - CORE Message Envelope and Metadata can also be used for non administrative Message Payloads

simplifying healthcare administration

CAQH®

Message Transport Layer: *Envelope Standards*

- CORE Connectivity supports two envelope standards to attach and send files
  - **HTTP MIME Multipart Messaging**
    - Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:
      - Text in character sets other than ASCII
      - Non-text attachments
      - Message bodies with multiple parts
      - Header information in non-ASCII character sets
    - Multipart/form-data is used to express values submitted through a form; it is most commonly used for submitting files via HTTP
  - **SOAP+WSDL**
    - SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information based on XML using web services
      - XML (Extensible Markup Language): meta-language that allows users to define their own customized way to describe data; language used in CORE Connectivity to create CORE specific metadata
    - Web Services Description Language (WSDL) is document written in XML to describe a Web service (software system to support machine-to-machine interactions over a network)

simplifying healthcare administration
CAQH®

Message Transport Layer: *Processing Modes/Interactions*

- CORE Connectivity addresses both batch & real-time processing modes and synchronous & asynchronous message interaction patterns
  - Processing Modes describe how message payload is processed

Processing Modes	Description
Real-time	• Entity sends single request, receives single response in real-time
Batch	• Entity submits batch of requests at the same time • Results of processing the batch of requests are sent back at a later time (i.e., not in real-time)

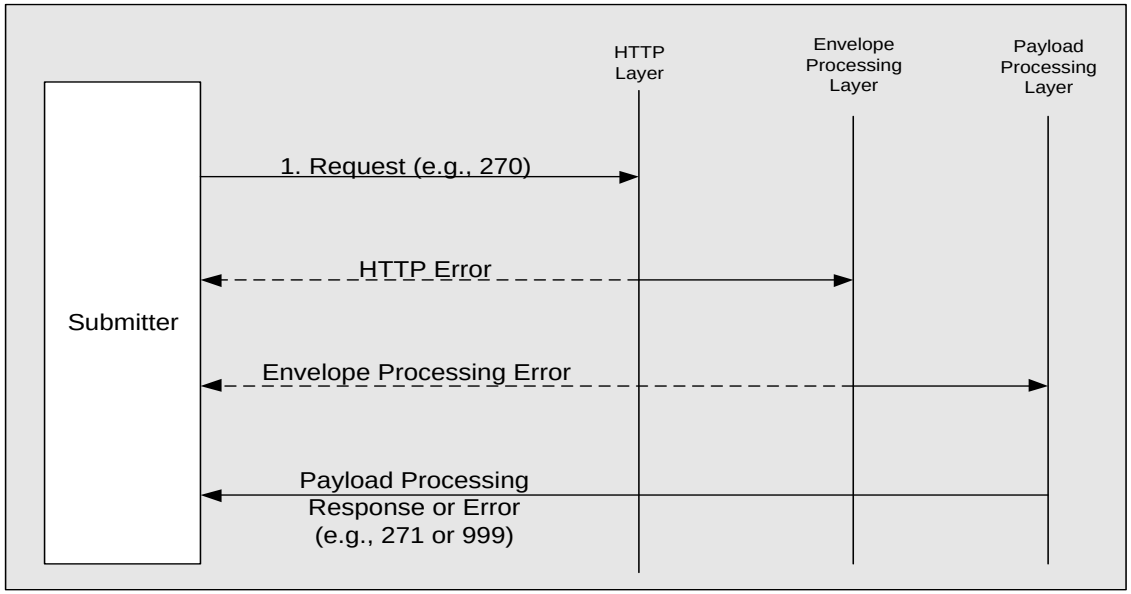
  - Message Interaction Patterns describe how connections are established and used for handling requests and responses

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 real-time mode of processing
Asynchronous	• Connection is established to send a request; response is sent on a separate connection • Typically associated with batch mode of processing

simplifying healthcare administration
CAQH®

CORE Connectivity: *Error Handling Across the Layers*

- Once request (e.g., X12 270) is submitted, it goes through 3 logical layers:
  1. Processing of HTTP headers (typically handled by a web-server)
  2. Processing the Envelope (can be handled by messaging middle-ware or integration brokers)
  3. Processing the Payload (e.g., ASC X12, typically handled by application business logic)
- At each layer, some part of request is processed and errors can be returned to submitter
  - If there is an error in processing message at any layer, request is not passed to the next layer
  - If no errors are encountered, request is passed to the next processing layer
  - Last logical layer that processes request is the Payload Processing Layer
  - Once payload is processed at Payload (Business) Processing Layer, it returns a response or error



simplifying healthcare administration
CAQH®

CORE Connectivity: *Security Across the Layers*

- Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over common medium of access
- CORE Connectivity Security Standards
  - Secure Socket Layer (SSL) 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
    - CORE Connectivity requires SSL 3.0 (and optionally TLS) for transport level security
      - Does not preclude optional use of TLS 1.0 (or higher version as required for FIPS 140 compliance) for connectivity with trading partners that require FIPS 140 compliance
  - For authenticating clients (i.e., “submitters”), one of two approaches is used:
    - X.509 Certificates over SSL (optionally, over TLS)
    - Username and Password (e.g., WS-Security Username Token in the SOAP option)
  - For payload integrity verification:
    - SHA-1 Checksum of the payload is sent as part of the message envelope
  - For reliability of transport:
    - UUID (Universally Unique Identifier) is used for Payload ID (for detecting duplicates)
    - Timestamp is used for ensuring that the data is recent

Q & A:

Questions on the Key Technical Concepts Addressed by CAQH CORE Connectivity

Additional Time for Q & A at the End of the Presentation

simplifying healthcare administration

CAQH®

Mandated CAQH CORE Connectivity Rules:

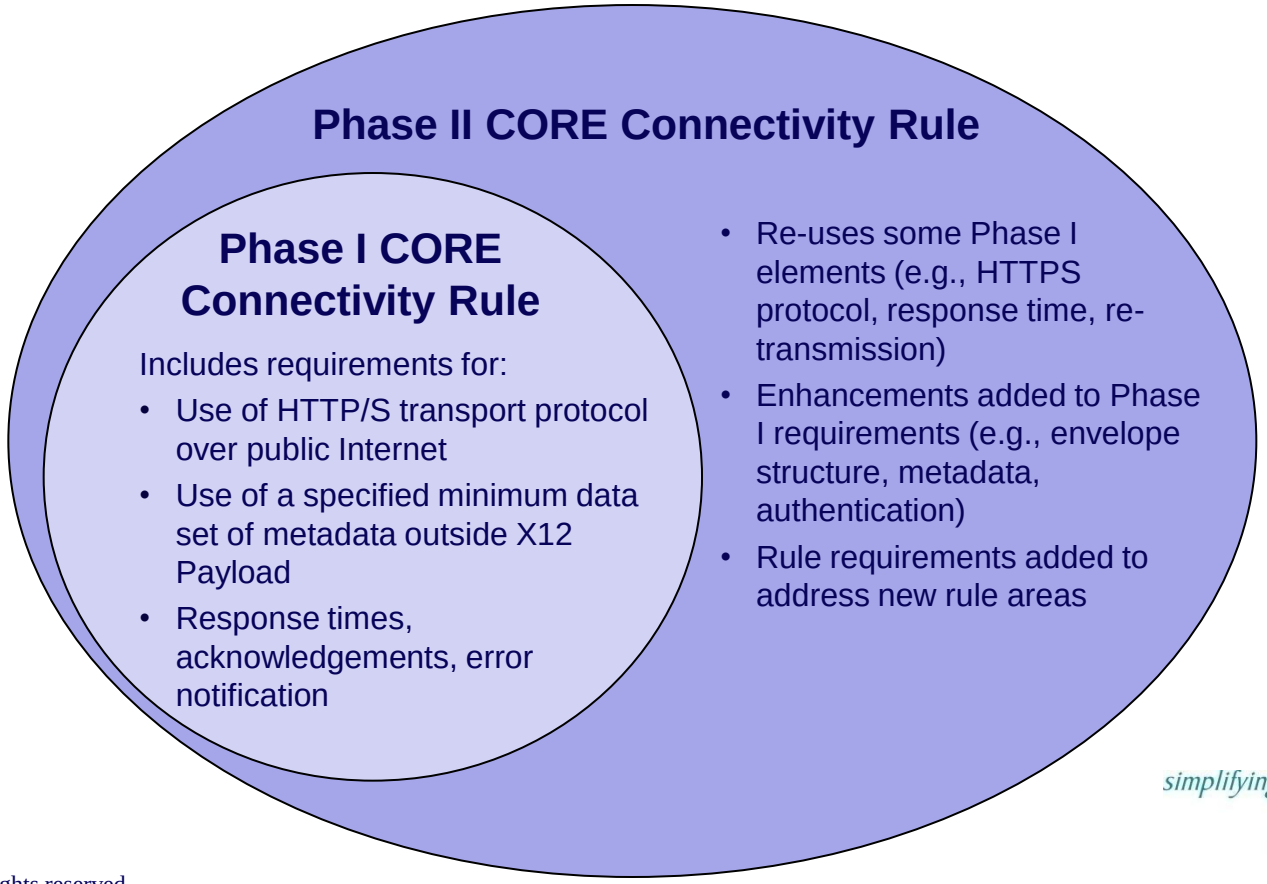
Detailed Rule Requirements

simplifying healthcare administration

CAQH

CORE Connectivity: *Rules Development*

- CORE Connectivity Rules were developed in phased, milestone drive approach
  - Phase I (CORE Rule 153) provided important first step & Phase II (CORE Rule 270) builds on Phase I foundation
  - All CORE Rule 153 requirements are incorporated into CORE Rule 270; *implementation of CORE Rule 270 incorporates all CORE Rule 153 requirements*



simplifying healthcare administration
CAQH®

CORE Connectivity: *Rules Development cont'd*

Technical criteria used by CORE Participants to develop the CORE Connectivity Rules

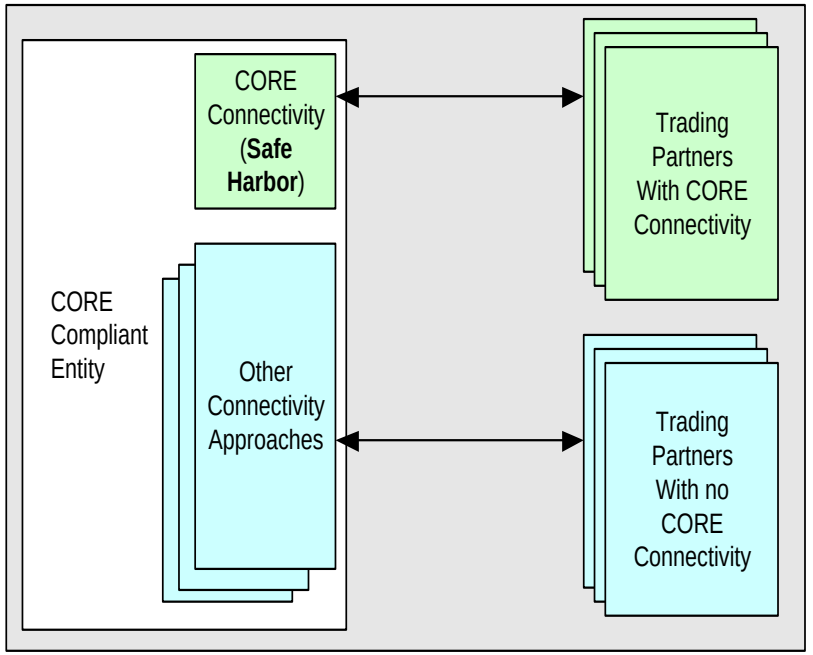
General Principles			
• Supports large batch transaction files with use of MTOM • Supports real-time transaction processing	• Supports large volume of single real-time transaction processing • Has extensive message attributes	• Supports synchronous & asynchronous message exchanges • Supports point-to-point message exchanges	• Supports push and pull messaging • Supports rules based routing

Security Principles	Reliable Messaging	Implementation Business Principles	Interoperability Principles
• Supports submitter authentication • Supports encrypted authentication • Supports digital certificate	• Payload independence • Message Metadata	• Language neutral • Platform neutral	• Compatible with emerging clinical standards for interoperability

simplifying healthcare administration
CAQH®

CORE Connectivity: *Safe Harbor Principle*

- Using the Internet as a delivery option, CORE Connectivity establishes "Safe Harbor" connectivity rule which standardizes flow of administrative transactions between health plan and provider
- As a "Safe Harbor":
  - Entities can be assured CORE Connectivity is implemented/supported by any trading partner
  - Trading partners always have a system that is interoperable between them
- CORE Connectivity "Safe Harbor" **DOES NOT** require:
  - Trading partners to remove existing connections that do not match the rule
  - Trading partners to use a CORE-conformant method for all new connections
  - All trading partners use only one method for all connections
  - Exclusive use of CORE Connectivity method (i.e., additional approaches can be used)
    - CORE Connectivity creates *a base and not a "ceiling"* - entities may offer additional connectivity interfaces



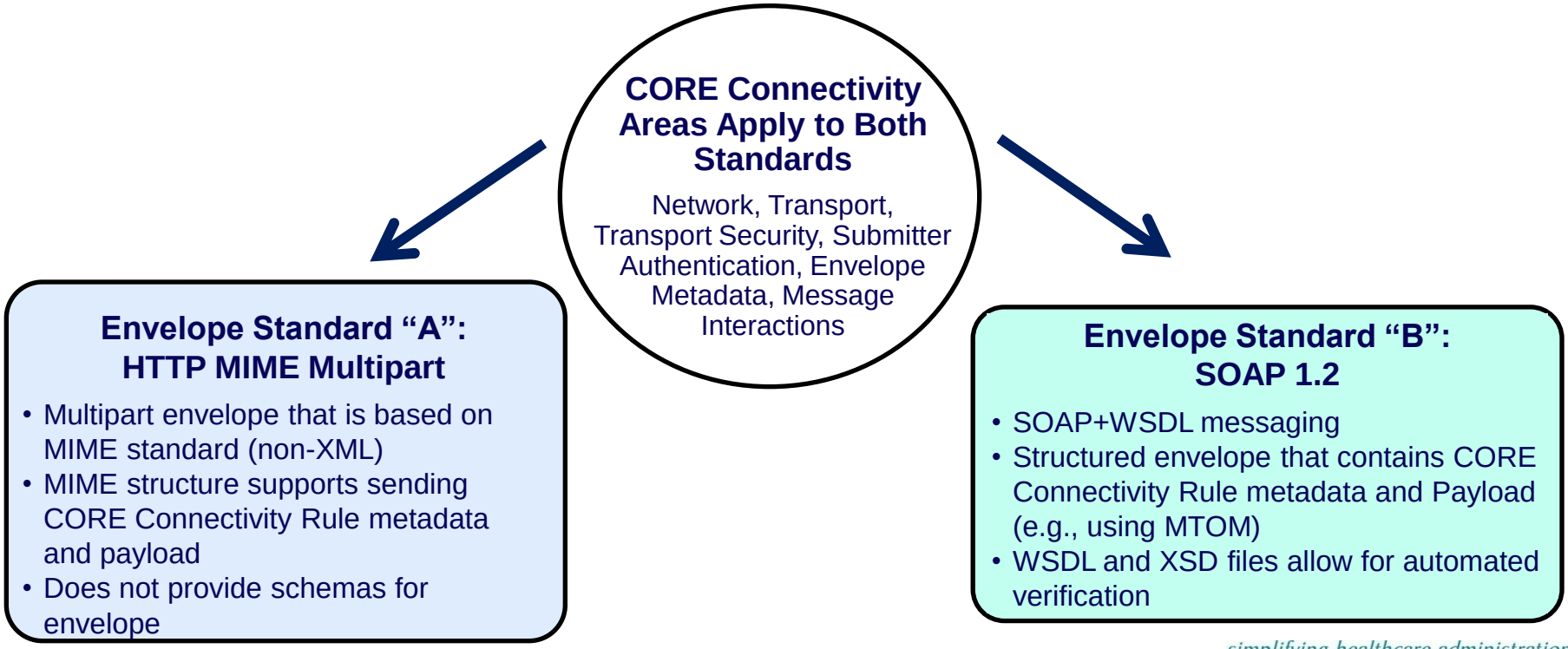
simplifying healthcare administration
CAQH

CORE Connectivity: *High-Level Rule Requirements*

Connectivity Rule Area	CORE Connectivity Rules
Network	Internet
Transport	HTTP
Transport Security	SSL, TLS (optional)
Submitter (Originating System or Client) Authentication	Name/Password X.509 Certificate (subject to conformance requirements)
Envelope and Attachment Standards	SOAP 1.2 + WSDL and MTOM (for batch) or HTTP+MIME (subject to conformance requirements)
Envelope Metadata	Metadata defined (field names, values) New PayloadTypes for HIPAA and non-HIPAA Payloads
Message Interactions/ Routing	Real-time required, batch optional (if entity performs batch processing, then batch mode processing for x12 270/271 and x12 276/277 must be supported)
Error Handling	Specifies error codes that must be returned for error conditions
Basic Conformance Requirements	Specifies for information sources performing role of HTTP/S server and information receivers performing role of HTTP/S client
Response Time	Real-time: Maximum response time from time of submission must be 20 seconds (or less) Batch: Response to transaction submitted by 9:00 pm E.T. must be returned by 7:00 am E.T. following business day
Companion Implementation Guide	Specific requirements for publication of entity-specific connectivity companion guide

CORE Connectivity Requirements: *Envelope Standards*

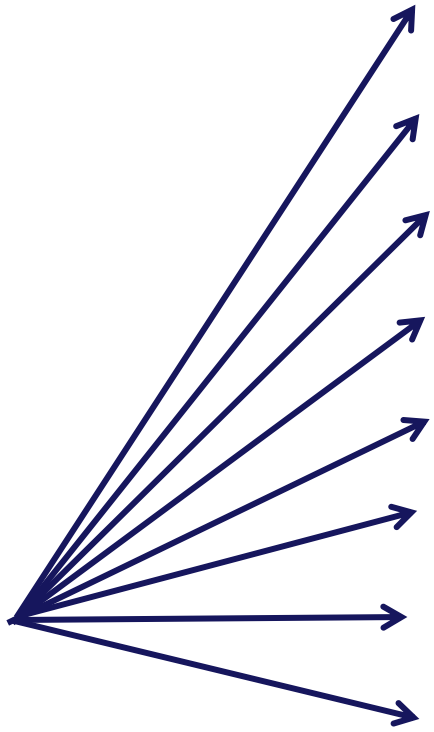
- CORE Connectivity supports two envelope standards, depending on stakeholder type
  - After extensive analysis, CORE Participants selected *HTTP MIME Multipart* & *SOAP + WSDL* as two standards that met majority of CORE technical criteria and had wide industry use
  - CORE Connectivity specifies SOAP envelope structure using XSD schemas and HTTP MIME envelope using examples
  - CORE Envelope Metadata is defined and consistent across either envelope standard



simplifying healthcare administration
CAQH

CORE Envelope Standard "A" (HTTP MIME Multipart): *Example*

- CORE Metadata in Use for HTTP MIME Multipart



CORE Envelope Metadata

Payload

```
POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Length: 2408
Content-Type: multipart/form-data; boundary=XbCY

--XbCY
Content-Disposition: form-data; name="PayloadType"

X12_270_Request_005010X279A1
--XbCY
Content-Disposition: form-data; name="ProcessingMode"

RealTime
--XbCY
Content-Disposition: form-data; name="PayloadID"

e51d4fae-7dec-11d0-a765-00a0c91e6da6
--XbCY
Content-Disposition: form-data; name="TimeStamp"

2007-08-30T10:20:34Z
--XbCY
Content-Disposition: form-data; name="UserName"

hospa
--XbCY
Content-Disposition: form-data; name="Password"

8y6dt3dd2
--XbCY
Content-Disposition: form-data; name="SenderID"

HospitalA
--XbCY
Content-Disposition: form-data; name="ReceiverID"

PayerB
--XbCY
Content-Disposition: form-data; name="CORERuleVersion"

2.1.0
--XbCY
Content-Disposition: form-data; name="Payload" filename="name.txt"

<contents of file go here -- 1674 bytes long as specified above>
--XbCY--
```

CORE Envelope Standard "B" (SOAP+WSDL): *Example*

- CORE Metadata in Use for SOAP Request

HTTP Headers

WS-Security Username & Password token

SOAP Envelope with remaining metadata from CORE Connectivity Rules

```
POST /core/eligibility HTTP/1.1
Host: server_host:server_port
Content-Type: application/soap+xml; charset=UTF-8; action="RealTimeTransaction"

<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
<soapenv:Header>
<wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true">
<wsse:UsernameToken xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd wsu:Id="UsernameToken-21621663">
<wsse:Username>bob</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">bobPW</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
 <soapenv:Body>
<ns1:COREEnvelopeRealTimeRequest xmlns:ns1="http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd">
                    <PayloadType> X12_270_Request_005010X279A1/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>2.2.0</CORERuleVersion>
 <Payload><![CDATA[ISA*00* *00* *ZZ*NEHEN780 *ZZ*NEHEN003 ...IEA*1*000000031]]></Payload>
</ns1:COREEnvelopeRealTimeRequest>
 </soapenv:Body>
</soapenv:Envelope>
```

CORE Connectivity Requirements: *Error Handling*

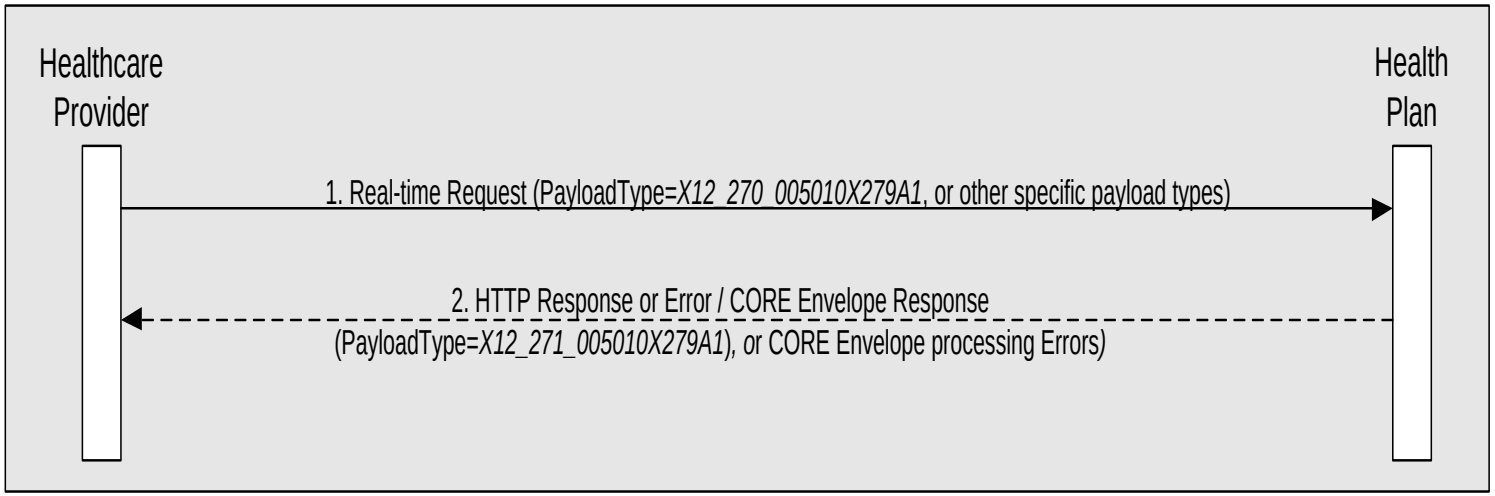
- CORE Connectivity addresses errors that can be returned at each logical layer

Error Type	Details
HTTP Status and Error Codes	• Rely upon the HTTP RFC 2616 for the specific and complete list of protocol specific errors that must be supported • CORE Connectivity Rules describe transport level status and error conditions and the use of HTTP status and error codes for those conditions
Envelope Processing Status and Error Codes	• Errors while processing the envelope (e.g., rule version mismatch) • Error codes are enumerated in CORE Connectivity Rule 270 • The intended use is defined in the rule documentation

simplifying healthcare administration
CAQH®

CORE Connectivity Requirements: *Processing Modes*

- Real-Time Processing Requirements
  - CORE Connectivity requires real-time (synchronous) processing for X12 270/271 and X12 276/277 transactions
  - Diagram illustrates real-time (synchronous) interaction between a provider and health plan



- Message Sequence 1: Provider submits real-time request to health plan using payload type as X12_270_Request_005010X279A1 or one of the specific payload types
- Message Sequence 2: Health plan responds (synchronously to message 1) with HTTP level error or HTTP successful response accompanied by CORE Envelope Level response (Payload type is X12_271_Response_005010X279A1 or error)

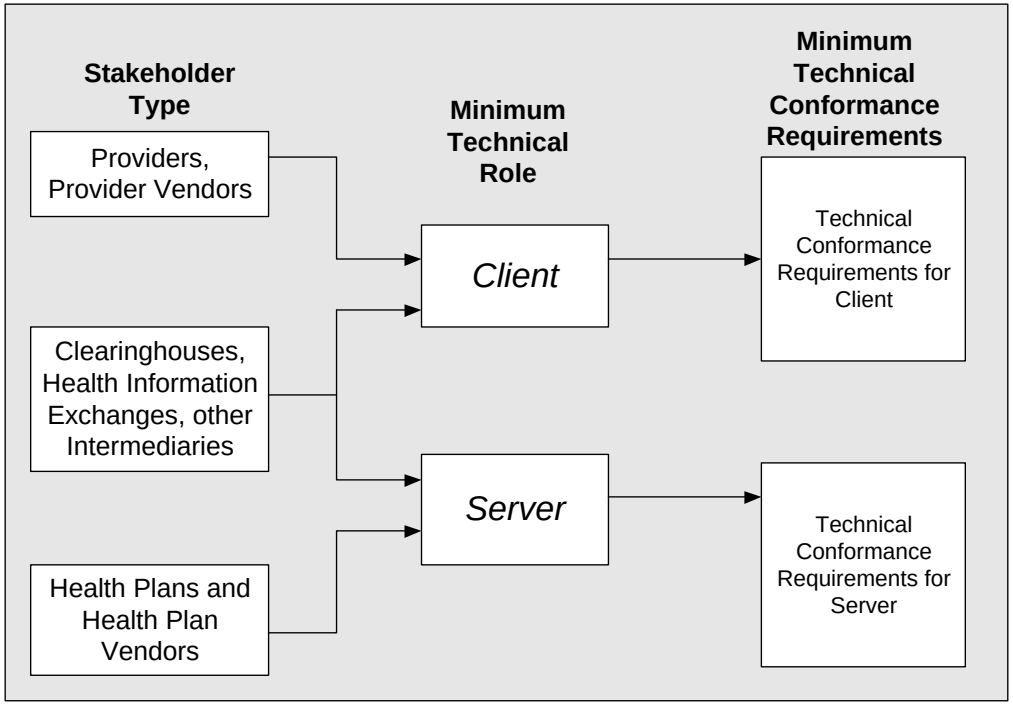
simplifying healthcare administration
CAQH

CORE Connectivity Requirements: *Processing Modes cont'd*

- Batch Processing Requirements
  - Batch (asynchronous) processing is ***optional*** for X12 270/271 and X12 276/277 transactions
  - ***However,*** if an entity performs batch processing, it must support batch processing for X12 270/271 and X12 276/277 transactions
  - There are a few defined interactions for batch processing within CORE Connectivity Rules:
    - Interaction can be conducted using specific or mixed payload types
    - Generic batch retrieval request and receipt confirmation
    - Generic batch submission with batch payload and synchronous payload receipt confirmation

CORE Connectivity: *Stakeholder Requirements*

- CORE Connectivity applies to information sources performing role of an HTTP/S server and information receivers performing role of an HTTP/S client
  - Rules define conformance requirements for stakeholders based on typical role (client, server) for envelope and authentication standards*
  - Diagram illustrates the typical (minimal) roles played by stakeholders (e.g., providers typically clients, health plans typically servers, clearinghouses can act as client or server)

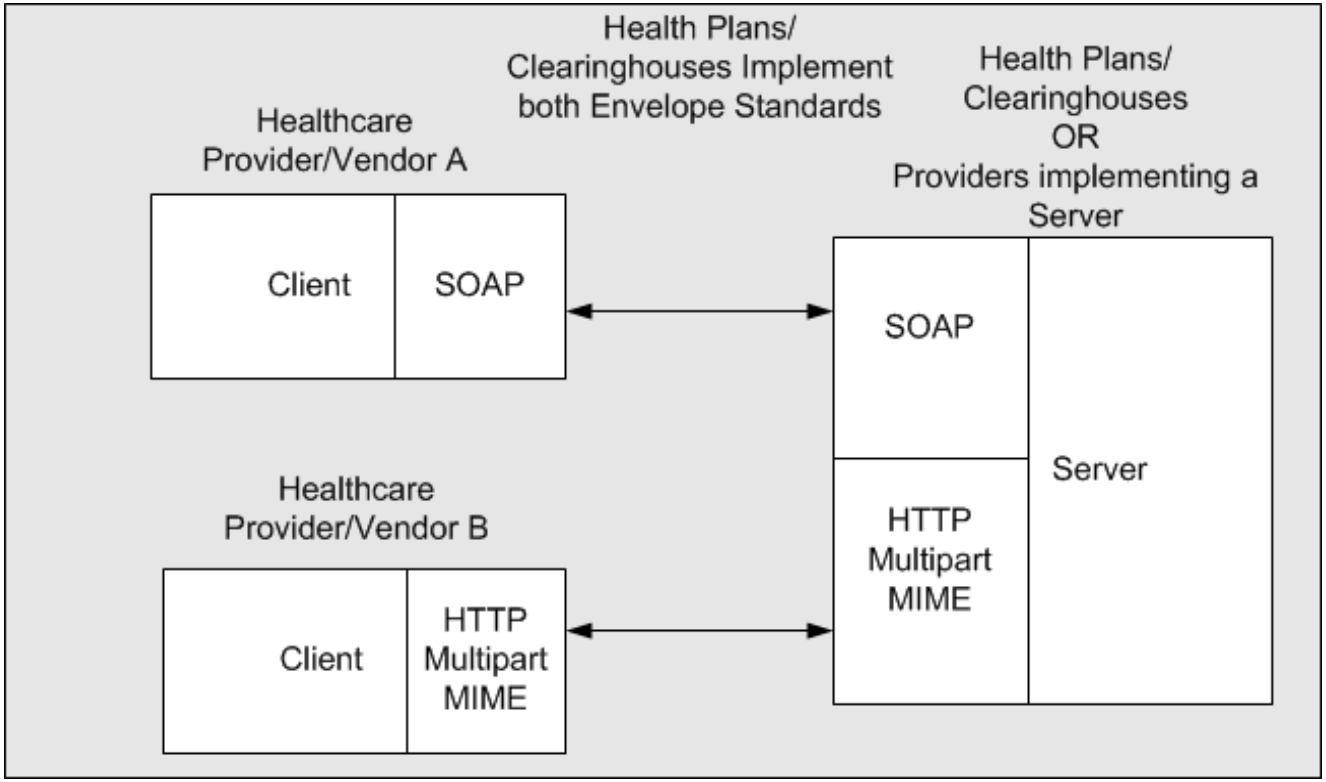


*See CORE Rule 270, Section 4.1 *Basic Conformance Requirements for Key Stakeholders* for detailed stakeholder requirements

simplifying healthcare administration CAQH

CORE Stakeholder Requirements: *Envelope Standards*

- Stakeholders in server role (e.g., health plans and clearinghouses/switches) must implement both envelope standards (SOAP+WSDL and HTTP MIME Multipart)
- Stakeholders in client role (e.g., healthcare providers or provider vendors) must implement one of the envelope standards, client can choose one of the two envelope standards

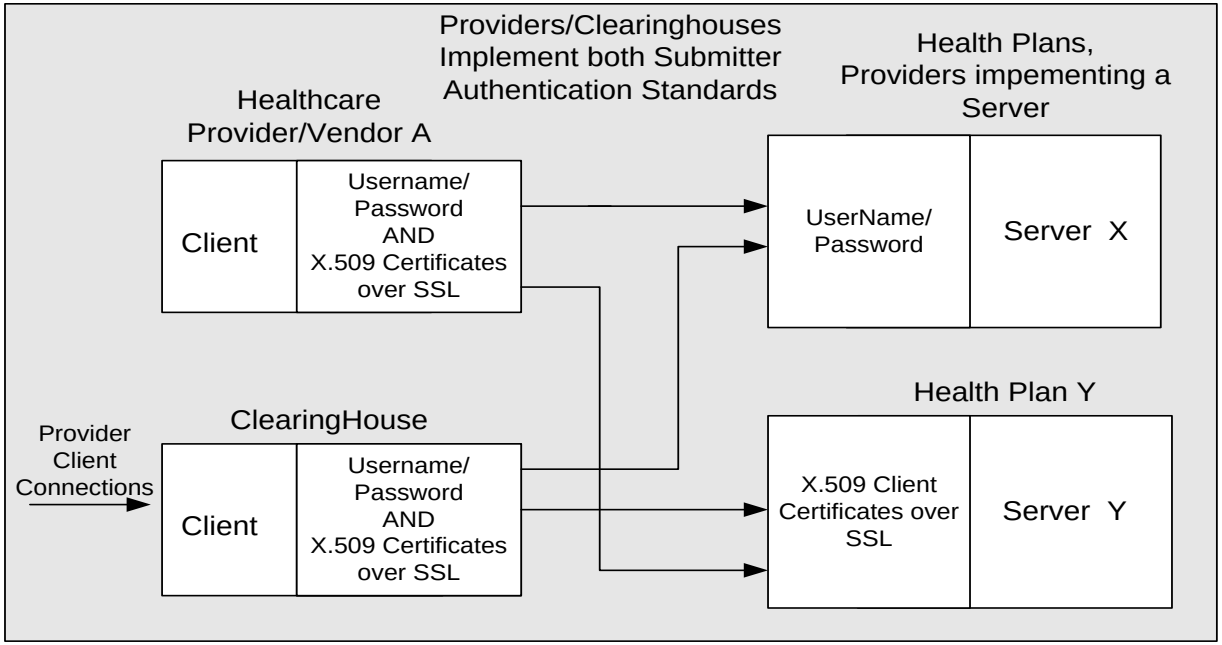


simplifying healthcare administration

CAQH

CORE Stakeholder Requirements: *Submitter Authentication*

- CORE Connectivity supports two methods for Submitter Authentication
  - Username/Password, using CORE-conformant Envelope to send CORE-conformant Envelope Metadata UserName and Password
  - X.509 Certificate based authentication over SSL standard for client certificate based authentication
- Stakeholders in server role (e.g., health plans) choose to implement one of the standards
- Stakeholders in client role (e.g., healthcare providers/provider vendors and clearinghouse components handling submissions to plans) must implement both standards



simplifying healthcare administration

CAQH

CORE Stakeholder Requirements: *Other Infrastructure*

- Response Time Requirements for Interactions
  - Servers must follow the requirements for response times for real-time interactions in CORE Real-Time Response Rule: CORE Rule 156
  - Servers must follow the requirements for response times for batch interactions as stated in CORE Batch Response Rule: CORE Rule 155
- Connectivity Companion Guide
  - If server organizations publish a Connectivity Implementation Companion Guide, the guide should be consistent with the guidelines for connectivity companion guides described in the CORE Connectivity Rules
  - CORE makes recommendations in CORE Connectivity Rules for specific topics and information in the connectivity companion guide

simplifying healthcare administration
CAQH®

Q & A:
Questions on the Detailed Requirements of the CAQH CORE Connectivity Rules

Additional Time for Q & A at the End of the Presentation

simplifying healthcare administration
CAQH

Implementing the Mandated CAQH CORE Connectivity Rules:

Perspectives from a CORE-certified Health Plan

David Querusio
Harvard Pilgrim Health Care, Inc.

simplifying healthcare administration
CAQH®

Harvard Pilgrim Health Care Overview

Harvard Pilgrim is the only private health plan in the nation to be named #1 for member satisfaction and quality of care for eight consecutive years according to an annual ranking of the nation's best health plans by the National Committee for Quality Assurance (NCQA)

- A regional not-for-profit health plan, based in Wellesley, MA
  - 1100 employees across 7 locations
  - Over one million members primarily in MA, NH, ME
  - Full range of health insurance choices, funding arrangements, and cost-sharing options
- A CAQH CORE Participating Organization
- Completed Phase I and II CORE Certification testing concurrently; a Phase I and II CORE-certified health plan

Harvard Pilgrim HealthCare

simplifying healthcare administration
CAQH

Harvard Pilgrim Channel Strategy: *Approach*

- Our Strategic Approach
  - Innovate or lead in adoption of channels or transactions
    - In 2003, created Healthcare Transaction Services (HTS), a new practice management system vendor channel based on existing EDI industry SOAP standards; handles ASC X12 270/271 and ASC X12 276/277 transactions
  - Increase trading partner choice over time
    - From two channels of connectivity for eligibility and claims status transactions in 2002 to seven channels supporting over 99% of transactions today
      - *NEHEN
      - *NEHEN Net (NEHEN add on)
      - *HTS
      - *HPHConnect*
      - *CORE SOAP
      - *CORE MIME
    - Channel and trading partner agnostic
    - Trading partners use multiple channels of connectivity depending on transaction type; e.g., EDI channel for high volume eligibility and *HPHConnect* for accounts receivable reconciliation (patient targeted eligibility and claims status inquiry)

Harvard Pilgrim HealthCare

simplifying healthcare administration CAQH

**CORE-enabled or CORE required*

Harvard Pilgrim Channel Strategy: *Why CORE?*

- Adoption of CORE rules was a natural next step as we continued to grow the Harvard Pilgrim "Channel Strategy"
- CAQH CORE Operating Rules
  - Support administrative simplification goals
  - Provide focused content standards
  - Provide common national connectivity standards – a clear fit for Harvard Pilgrim with one of the CORE connectivity standards based on the same SOAP standards used in our HTS channel
  - Provide additional opportunities to meet different trading partner technology capabilities

Harvard Pilgrim Health Care

simplifying healthcare administration CAQH

Harvard Pilgrim: *Technology Stack*

- Harvard Pilgrim chose commonly available software products in the industry, i.e., open source libraries and technology
- Selected an application portfolio that helped us meet both industry technical standards and CAQH CORE Infrastructure Operating Rules, i.e.,
  - WebLogic Application Server
  - Apache Axis2 Version 1.4 running under WebLogic
  - Java Version 6.0
  - Apache Commons File Upload Utility
  - Castor Version 1.2
  - Java interface with TIBCO Rendezvous

Harvard Pilgrim HealthCare

simplifying healthcare administration CAQH

Harvard Pilgrim: *Design Approach*

The design approach to implementing CORE Connectivity key requirements was as follows:

- **SOAP Channel**
  - Apache HTTP Server running on a Linux machine in the DMZ receives the request, decrypts it and routes it to the SOAP end-point hosted in WebLogic server
  - Apache Axis2 processes the SOAP messages
  - Data binding is done using the open-source Castor
- **MIME-Multipart Channel**
  - Apache HTTP Server running on a Linux machine in the DMZ receives the request, decrypts it and routes it to the MIME end-point hosted in WebLogic server
  - Apache File Upload is used as the multi-part parser
  - Data binding is done using the open-source Castor
- **Security**
  - Apache Server in the DMZ does the client authentication using X.509 client certificates over SSL

Harvard Pilgrim HealthCare

simplifying healthcare administration CAQH®

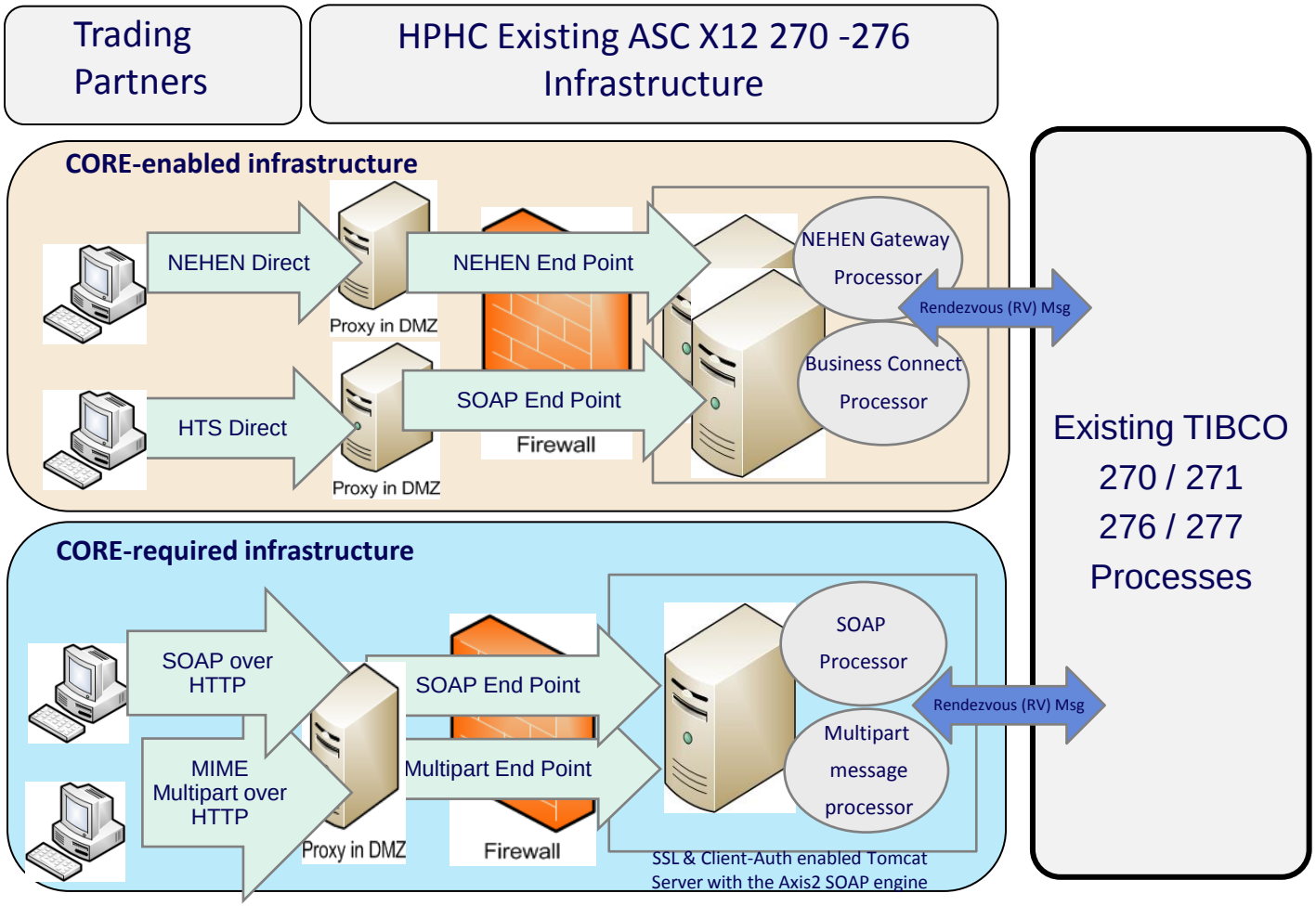
Harvard Pilgrim: *Design Approach cont'd*

- One of the design goals was to leverage the existing processes and infrastructure
- At a high level, here were the different steps involved:
  - Two new end-points (URLs) were configured in the external-facing Apache-server in the DMZ, one for each of the new channels; this server routes the incoming requests to the SOAP & MIME end-points hosted in WebLogic
  - Apache server was configured for client-certificates; providers are issued certificates by HPHC in order for them to be able to connect to Harvard Pilgrim over HTTPS
  - Apache server decrypts the incoming request and routes it to the appropriate end-point in WebLogic, passing in the credentials from the client-cert
  - The WebLogic application extracts the data from the HTTP request, including the client-cert credentials to do authorization; it then sends the EDI-payload as a message to the existing back-end infrastructure for real-time transactions; for batch, it streams the X12 payload to a file-system on the disk that is used by the existing batch processing infrastructure
  - Using this design approach, HPHC was able to achieve CORE compliance with minimal impact to the existing processes used by the other non-CORE channels

Harvard Pilgrim HealthCare

simplifying healthcare administration CAQH

Harvard Pilgrim: *EDI Infrastructure*



Harvard Pilgrim HealthCare

simplifying healthcare administration CAQH

The Harvard Pilgrim Experience:
CORE Connectivity Implementation Challenges

- Availability of Skilled Resources
  - *Challenge:* Key resources had little experience with MIME and MTOM attachments
  - *Solution:* We trained developers and sought examples online
- Data Mapping
  - *Challenge:* Mapping to standard codes proved tedious and challenging; process brought to light other data issues
  - *Solution:* Take time to understand the data mappings; work closely with data analysts
- Certificate Management
  - *Challenge:* Certificate management can be a challenge; certificates expire every year; certificates are stored and managed differently on windows versus Linux, and .net versus Java application servers
  - *Solution:* Developed a how-to document to help developers
    - Participated in CORE Connectivity PKI Pilot which streamlines certificate management and reduces the complexity associated with multiple Certificate Authorities

The Harvard Pilgrim Experience:
Improvement in Patient and Provider Experience

- Reduced claim rejections and denials related to eligibility (~ 35% reduction)
- Improved efficiency and growth in trading partner interactions
  - Five (5) trading partners, all vendors, now live with CORE Connectivity
    - Care Core National, Health Management Systems, HealthTrio, Recondo Technologies & The SSI Group
  - While all had reduced turn around time from previous enrollments – had a record 15 business day turn-around for implementation with a CORE-certified vendor; 1/4 to 1/3 length of previous implementations (40 - 60 business days for X12 270 or X12 276 with other trading partners)
  - Greater growth in these vendors' use of transactions compared to EDI overall
    - Included decline in overall EDI claims status inquiry rates
    - CORE Connectivity use increased 6-fold
- Monthly eligibility tracking by a national application service vendor has reported Harvard Pilgrim eligibility accuracy greater than aggregated national commercial rate*

Harvard Pilgrim Health Care

*__NOTE__: Based on application vendor data; CORE Rules do not guarantee accuracy of information

simplifying healthcare administration CAQH®

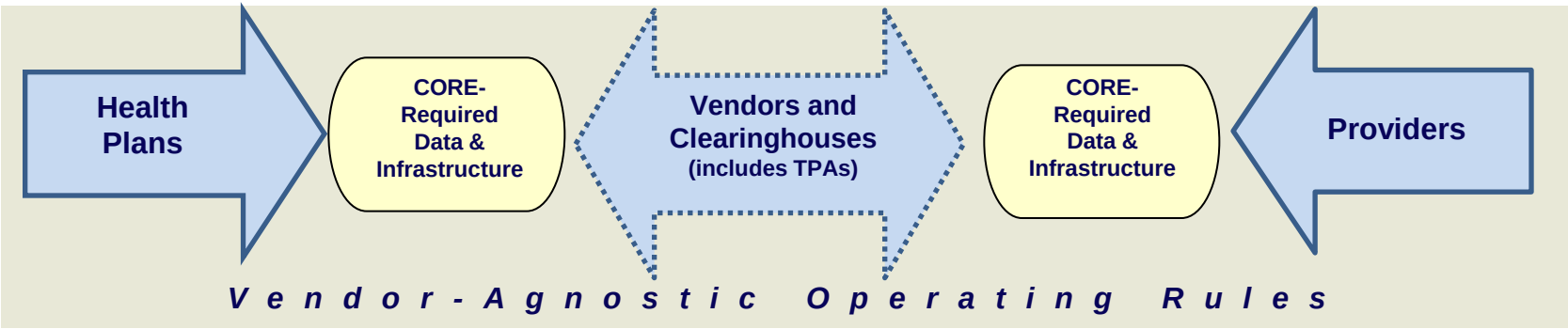
30-Second Poll:
Your Organization's Most Challenging CAQH CORE Connectivity Rule Requirement

simplifying healthcare administration
CAQH

Implementing the Mandated CAQH CORE Connectivity Rules: *Additional Guidance*

simplifying healthcare administration
CAQH®

CORE Connectivity Implementation:
Multi-stakeholder Connectivity



- All HIPAA covered entities work together to exchange transaction data in a variety of ways (i.e., providers, health plans, clearinghouses)
- Understand electronic data flows associated with your administrative agreements
- When clearinghouse or vendor is involved in data exchange between health plan and provider eligibility systems, then:
  - Identifying end-to-end role and responsibility of each entity is an important step
  - Each entity will be responsible for their own specific implementation, testing, and related resources
  - Joint integration planning between entities will ensure conformance requirements and Return on Investment (ROI) goals are met

simplifying healthcare administration
CAQH®

CORE Connectivity Implementation: *Key Considerations*

Implementation of CORE Connectivity will vary based on your organization's characteristics

High-Level Planning Questions	Possible Considerations
1. Do you use systems impacted by the CORE Connectivity Rules?	• Do you have an in-house system or an outsourced connectivity solution? • If outsourced, determine implementation/compliance timeline of your vendor.
2. Should you build or buy CORE-conformant connectivity interfaces for the administrative transactions?	• Build or buy decisions will be influenced by organization characteristics such as level of comfort with outsourcing or ability to accomplish an in-house implementation • Consider using CORE-conformant vendors and clearinghouses that already have CORE-conformant interfaces available for use
3. What is your stakeholder type and how does it map to the client or server technical roles relative to connectivity?	• Do you connect with trading partners as a client, or as a server, or both? • Depending on this, consider the minimum technical requirements based on the conformance requirements detailed in the CORE Connectivity Rules
4. What gaps exist between what you have and what you need?	• Perform gap analysis of current systems against technical CORE Connectivity requirements
5. What is the workload and planning necessary to deliver for the Federal deadline?	• Work backward from implementation deadlines to understand the level of effort needed for your organization to remain compliant
6. Do you wish to transition your trading partners to the new connectivity approach? What is your transition plan?	• Consider client notifications that will be necessary and how long it may take clients to switch to the new interfaces • Provide test environments as early as possible for clients to understand updates
7. What internal groups need to be notified of these changes? Have you aligned your implementation plan with your organization's internal architecture body?	• Depending on your security solutions, CORE Connectivity may require additional reviews from internal security groups to make sure it meets your needed requirements • Conduct architectural review and joint application design session

CORE Connectivity Implementation: *Voluntary CORE Certification

- Consider pursuing voluntary CORE Certification
  - **WHY:** CORE Certification testing offers a mechanism to test your ability to exchange eligibility and claim status transaction data with your trading partners
- Key benefits of voluntary CORE Certification
  - Demonstrates to the industry adoption of the CAQH CORE Operating Rules via a recognized industry "Seal" due to multi-stakeholder collaboration
  - Encourages trading partners to work together on transaction data content, infrastructure and connectivity needs
  - Independent testing of operating rules implementation can reduce the amount of work required for successful trading partner testing
  - Promotes maximum ROI when all stakeholders in the information exchange are known to conform with the CAQH CORE Operating Rules
- Currently, 58 organizations/products CORE-certified
- Certification and testing are *separate activities*
  - Testing is performed online by CAQH CORE-authorized testing vendor; Certification is completed by CAQH CORE and occurs after successful testing is completed

***NOTES:**

1. The voluntary CORE Certification Program offered by CAQH CORE is separate from the HHS-required health plan certification program mandated by the ACA. Information on the CMS compliance program regarding operating rules is under development and can be found HERE.
2. Entities are required to complete the rule requirements pertaining to Acknowledgements to achieve *voluntary* CORE Certification.

simplifying healthcare administration CAQH®

30-Second Poll:
Connectivity Education Session Evaluation

Send Additional Questions &/or Feedback to CORE@caqh.org

simplifying healthcare administration
CAQH

Question & Answer

Send Additional Questions &/or Feedback to CORE@caqh.org

simplifying healthcare administration
CAQH

Appendix:

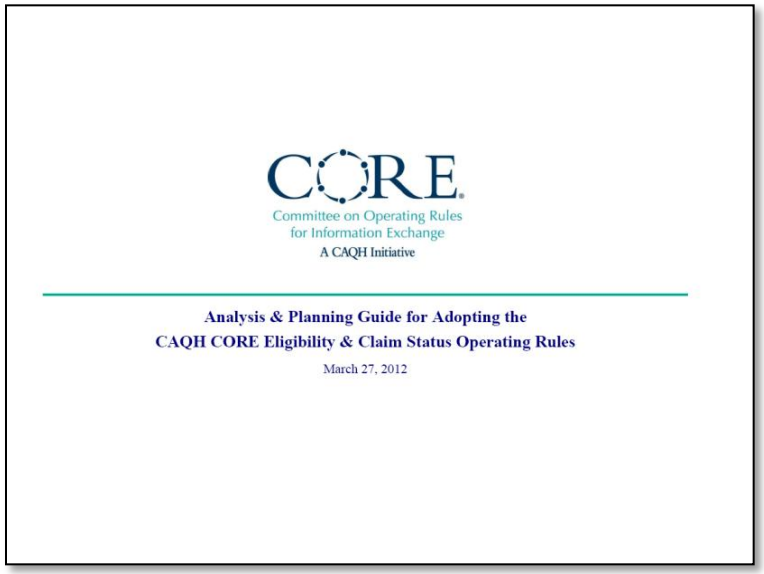
CAQH CORE Resources for Implementing the Mandated CAQH CORE Connectivity Rules

simplifying healthcare administration

CAQH

CORE Connectivity Implementation: *Resources*

- New *Analysis & Planning Guide for Adopting the CAQH CORE Eligibility & Claim Status Operating Rules* provides guidance for Project Managers, Business Analysts, System Analysts, Architects, and other project staff to complete systems analysis and planning



Guide should be used by project staff to:

- Understand applicability of the CAQH CORE Operating Rule requirements to organization's systems that conduct the eligibility and/or claim status transactions
- Identify all impacted external and internal systems and outsourced vendors that process eligibility and/or claim status transactions
- Conduct detailed rule requirements gap analysis to identify system(s) that may require remediation and business process which may be impacted

- Includes three tools to assist entities in completing analysis and planning:
  - Stakeholder & Business Type Evaluation
  - Systems Inventory & Impact Assessment Worksheet
  - Gap Analysis Worksheet

simplifying healthcare administration
simplifying healthcare administration
CAQH

CORE Connectivity Implementation: *Resources cont'd*

- *FAQs*:
  - CAQH CORE has a list of FAQs to address typical questions regarding the operating rules; in the process of reviewing these FAQs and updating as appropriate given mandates
    - **Example: FAQ #263: *CAQH CORE 270: Username and Password Guidelines***
      - **Question:** Are there any guidelines/restrictions on the Username and Passwords that can be used?
      - **Answer:** The length of username and password should not exceed 50 characters. Beyond this, CORE Connectivity Rule 270 does not specify guidelines/restrictions on the username and passwords.
    - If question not listed as an FAQ, email question to CORE@caqh.org
- *Phase I & Phase II CORE Certification Master Test Suites*:
  - Initially developed for voluntary CORE Certification but same concepts, e.g., role of trading partners, apply for general adoption of the CAQH CORE Operating Rules
- *Education Sessions*:
  - CAQH CORE holds frequent sessions with partners (WEDI, CHIME, Medicaids) and many include speakers from organizations that have already implemented the rules; upcoming and past CAQH CORE Education Sessions available HERE
  - Upcoming Public CAQH CORE Town Halls (click to add to Outlook Calendar)
    - July 24th, 3:00-4:00 pm ET
    - September 11th, 3:00-4:00 pm ET
- *General/Interpretation Questions*:
  - After reviewing other tools & resources, email CORE@caqh.org for additional interpretations or general questions

simplifying healthcare administration
simplifying healthcare administration
CAQH