Alignment of CAQH CORE, ACA Section 1104, NwHIN and esMD

August 29, 2012

Raja Kailar
Business Networks International (BNETAL)
(CAQH CORE Consultant)

Rachel Foerster
Boundary Information Group
(CAQH CORE Consultant)

This document is for educational purposes only; in the case of a question between this document and CAQH CORE Operating Rule text and/or Federal regulations, the latter take precedence.
Outline

• Federally Mandated Implementation Base of CAQH CORE Rules (5 min)

• NwHIN, and esMD in Context of CAQH CORE Connectivity Rules (10 min)
  – Incorporation of CAQH CORE Connectivity Rule into NwHIN and esMD Specifications
  – Potential use of CAQH CORE Connectivity Rule to further support esMD

• Mandated CAQH CORE Connectivity Operating Rules (25 min)
  – Guiding principles to enhance interoperability and alignment
  – Technical requirements
  – Change/Maintenance Process
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.

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.

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.

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.
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
ACA Section 1104 Administrative Simplification and Federally Mandated Operating Rules

• ACA Section 1104 requires Secretary of Health and Human Services (HHS) to adopt and regularly update operating rules for **three sets** of healthcare administrative transactions
  – First set addresses Eligibility for a Health Plan and Health Care Claim Status transactions (Compliance date for HIPAA covered entities: January 1, 2013)
    • December 2011: HHS **adopted** the CAQH CORE Eligibility & Claim Status Operating Rules to fulfill the Federal mandate, *with the exception of requirements for Acknowledgements and voluntary CORE Certification*
  – Second set addresses Health Care Electronic Funds Transfers (EFT) and Remittance Advice transactions (Compliance date for HIPAA covered entities: January 1, 2014)
    • August 2012: HHS **proposed** the CAQH CORE EFT & ERA Operating Rules via an Interim Final Rule with Comment (IFC), *with the exception of one requirement for use of acknowledgements*
  – Third set addresses enrollment, prior authorization, attachments, etc. (Compliance date for HIPAA covered entities: January 1, 2016)
    • No regulations have been released related to the third set of operating rules; CAQH CORE has been recommended, has done research and will be launching formal rule development activities

• 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
  – CAQH CORE **overview** of the Federally mandated operating rules (including implementation resources for eligibility & claim status rules) and links to and [complete CAQH CORE rule sets](#) and related [education sessions](#)

Note: ACA amends HIPAA.
### Federally Mandated Eligibility & Claim Status Operating Rules: **Scope**

<table>
<thead>
<tr>
<th>Type of Rule</th>
<th>Addresses</th>
<th>CAQH CORE Eligibility &amp; Claim Status Operating Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Content: Eligibility</strong></td>
<td>Need to drive further industry value in transaction processing</td>
<td>More Robust Eligibility Verification Plus Financials</td>
</tr>
<tr>
<td><strong>Infrastructure: Eligibility and Claim Status</strong></td>
<td>Industry needs for common/accessible documentation</td>
<td>Companion Guides</td>
</tr>
<tr>
<td></td>
<td>Industry-wide goals for architecture/performance/connectivity</td>
<td>Response Times</td>
</tr>
</tbody>
</table>

*Please Note: In the Final Rule for *Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction*, CORE 150 and CORE 151 are not included for adoption. HHS is not requiring compliance with any operating rules related to acknowledgement, the Interim Final Rule.*

---

**Acknowledgements**

“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.”

*HHS Interim Final Rule*
Federally Mandated CORE Infrastructure Rules

- **CORE Connectivity requirements**
  - Clients and Servers must follow the requirements in CORE Rule 270 and CORE Rule 153.

- **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

- **System Availability Requirements**
  - Servers must follow the requirements for system availability requirements in CORE System Availability Rule: CORE Rule 157

- **Companion Guide**
  - Servers must publish detailed specifications in a Connectivity Companion Guide. The guide should be consistent with the guidelines for companion guides described in the CORE Connectivity Rule 270
  - CORE makes recommendations in CORE Connectivity Rule 270 for specific topics and information in the Companion Guide
NwHIN and esMD in Context of CAQH CORE Connectivity Rules
Background

- **CAQH CORE 270 Connectivity Rule** is part of Eligibility and Claim Status Operating Rule set required by Administrative Simplification Provisions of ACA Section 1104
  - CORE Connectivity Rule is payload agnostic, and can transport any Payload, including both X12 and non-X12.
  - ACA Section 1104 applies to HIPAA covered entities including Health Plans, Medicare and State Medicaid, and thus adoption by these entities is required
  - **CAQH CORE 270 Connectivity Rule** supports SOAP 1.2 over the public Internet

- **NwHIN Service Interface Specification: CAQH CORE X12 Document Submission Specification** for administrative transactions (i.e., all X12 Payloads) has adopted CORE 270 Connectivity Rule for use over NwHIN
  - e.g., esMD Phase I X12 Profile uses the **NwHIN Service Interface Specification: CAQH CORE X12 Document Submission Specification**

- Together, **CAQH CORE 270 Connectivity Rule** and **NwHIN Service Interface Specification: CAQH CORE X12 Document Submission** provide a connectivity and security approach for both public and private sector use.
Aligned Building Blocks for Enabling Complementary Missions and Visions

CMS esMD Phase I
X12 Profile

Applies NwHIN Service Interface Specification to Submission of esMD (X12 275)

NwHIN Service Interface Specification:
CAQH CORE X12 Document Submission Service Interface Specifications v 1.0 (3/6/2012)

Defines NwHIN Constraints like SOAP, SAML, TLS

Part of set of Operating Rules Federally Mandated as part of ACA Section 1104

CAQH CORE 270 Connectivity Rule 2.2.0
CAQH CORE 270 Connectivity Rule 2.2.0, NwHIN CAQH CORE X12 Document Submission Specification and esMD X12 Profile: Layered View
Layered View of ASC X12 and CAQH CORE Connectivity Rule Message Envelope
NwHIN Constraints on CAQH CORE Connectivity Rule for CMS esMD Phase I: X12 Profile Payload and Message Envelope Layers
*Current and Future Use Cases for esMD*

**INBOUND**
- 2011
  - Responses to Documentation Request Letters in PDF/XDR format
- 2012
  - **Response to Documentation Request Letters in PDF/X12 format**
  - Appeal Requests in PDF
  - Advance Determination of Medicare Coverage (ADMC) Requests in PDF
  - Unsolicited Documentation in PDF (called paperwork or “PWK”)
- 2013
  - Structured Orders with author-level cryptographic verifiable signature
  - Structured Progress Notes with author-level cryptographic verifiable signature
  - Structured esMD Phase 2 Registration with author-level cryptographic verifiable signature

**OUTBOUND**
- 2013
  - Structured Outbound Documentation Requests
- 2014
  - Review Results Letters
  - Demand Letters

**LOOKUP**
- Request\Receive Documentation Status
- Request\Receive Claim Status
- Request\Receive Appeals Status
- Request\Receive Eligibility Info

---

*Slide from testimony to NCVHS by Melanie Combs Dyer (CMS), Fall 2011*
Federally Mandated CAQH CORE Connectivity Rules: 
*Enhancing the Interoperability and Alignment*
CAQH CORE Connectivity Rules: *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

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

- When a clearinghouse or vendor is involved in data exchange between the health plan and the provider’s eligibility systems, then:
  - Identifying the role and responsibility of each entity from an end-to-end perspective is an important step
  - Each entity will be responsible for their own specific implementation, testing and related resources
  - Joint integration planning between HIPAA covered entities and their vendors will ensure that conformance requirements and return on investment (ROI) goals are met
- CAQH CORE Connectivity Rules represent a minimum level of requirements (i.e., a base and not ceiling).
  - Entities may go above and beyond the rules to ensure the implementations meet their needs.
CAQH CORE Connectivity: *Industry Evolution*

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

**Phase I CAQH CORE Connectivity Rule:** Standardized Transport

**Phase II CAQH CORE Connectivity Rule:** 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

Prior to CAQH CORE Connectivity Rules: No Uniform Connection Standard

Costly management of multiple protocols, many proprietary

Greater online access due to uniformity in transport protocols
CAQH CORE Alignment With Federal Health IT Efforts

- CAQH CORE has sought and continues to seek alignment with major federal health IT initiatives in order for industry to leverage investments/ incentives to drive industry adoption.
- Major initiatives have recognized CAQH CORE rules and/or are working with CAQH CORE.
- As HIT complexities grow and market adoption becomes a reality, alignment continues to be critical.

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Nationwide Health Information Network (NwHIN)</td>
</tr>
<tr>
<td>2007</td>
<td>HITECH / Meaningful Use</td>
</tr>
<tr>
<td>2008</td>
<td>Healthcare Information Technology Standards Panel (HITSP)</td>
</tr>
<tr>
<td>2009</td>
<td>ONC S&amp;I Framework</td>
</tr>
<tr>
<td>2010</td>
<td>CMS esMD</td>
</tr>
<tr>
<td>2011</td>
<td>American Health Information Community (AHIC; now NeHC)</td>
</tr>
<tr>
<td>2012</td>
<td>ACA</td>
</tr>
<tr>
<td>2013</td>
<td>HIPAA 5010</td>
</tr>
<tr>
<td>2013</td>
<td>ICD-10</td>
</tr>
</tbody>
</table>

CAQH CORE Phase I → Phase II → Phase III
CAQH CORE Connectivity Rules: 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 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
  - CAQH CORE Connectivity Rules are designed to align with NwHIN; future rules will continue alignment

- CMS Electronic Submission of Medical Documentation (esMD) Program
  - CAQH 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

- Close coordination with other key health IT efforts including ONC S&I Framework, HITSP, NeHC, etc.
CAQH CORE Connectivity Rules: *Example Technical Criteria used for Development*

### General Principles

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports large batch</td>
<td>Supports large volume</td>
<td>Supports synchronous &amp;</td>
<td>Supports push and pull</td>
</tr>
<tr>
<td>transaction files with use</td>
<td>of single real-time</td>
<td>asynchronous message</td>
<td>messaging</td>
</tr>
<tr>
<td>of MTOM</td>
<td>transaction processing</td>
<td>exchanges</td>
<td></td>
</tr>
<tr>
<td>Supports real-time</td>
<td>Has extensive message</td>
<td>Supports point-to-point</td>
<td></td>
</tr>
<tr>
<td>transaction processing</td>
<td>attributes</td>
<td>message exchanges</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Security Principles

| Supports submitter           | Supports encrypted            | Supports digital             |                              |
| authentication               | authentication                | certificate                  |                              |

### Reliable Messaging

| Payload independence        | Message Metadata              | Language neutral             |                              |
| Message Metadata             |                              | Platform neutral             |                              |

### Implementation Business Principles

### Interoperability Principles

| Compatible with emerging   |
| clinical standards for     |
| interoperability            |
CAQH CORE Connectivity Rules: Safe Harbor Principle

- The CAQH CORE Connectivity Rule Safe Harbor requirements that a HIPAA Covered Entity (Health Plan) must support are described in CAQH CORE Rule 270 Section 5, CORE Safe Harbor.
- The CAQH CORE Connectivity Rule Safe Harbor specifies connectivity methods 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 the request by a Covered Entity to exchange data using the CAQH CORE Connectivity Rule.
- As a “Safe Harbor” the CAQH CORE Connectivity Rule ensures:
  - HIPAA Covered Entities can be assured CAQH CORE Connectivity Rule is implemented/supported by any covered entity
  - Covered Entities always have a system that is interoperable between them
- CAQH CORE Connectivity Rule “Safe Harbor” **DOES NOT** require:
  - HIPAA Covered Entities to remove existing connections that do not match the rule
  - HIPAA Covered Entities to use a CORE-conformant method for all new connections
  - All HIPAA Covered Entities to use only one method for all connections
- CAQH CORE Connectivity Rule creates a *base and not a “ceiling”* – HIPAA Covered Entities may offer additional connectivity interfaces

- In some circumstances, HIPAA Covered Entities may decide to continue to use current connections; however all HIPAA Covered Entities must implement the capability to use the CAQH CORE Connectivity Rule Safe Harbor and be capable and ready to use it when requested.
Federally Mandated CAQH CORE Connectivity Rules: 
*Key Technical Concepts*
CAQH CORE Connectivity Rules: Technical Standards

- CAQH 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
- CAQH 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
CAQH CORE Connectivity Rules: *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
CAQH CORE Connectivity Rules: *Layered View cont’d*

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

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

- **Message Transport Layer:**
  - CAQH CORE Connectivity Rules prescribe use of a securely encrypted Message Transport Layer
    - Rules require HTTP over SSL; CAQH CORE Connectivity Rule 270 includes optional use of TLS
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
- **CAQH 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 CAQH CORE Connectivity, Message Envelope consists of a well-defined structure for organizing and formatting Message Envelope Metadata
  - CAQH CORE Message Envelope Metadata help message receivers route messages for internal processing without opening envelope, reducing costs and improving response time
  - CAQH CORE Message Envelope and Metadata can also be used for non administrative Message Payloads
Message Transport Layer: *Envelope Standards*

- CAQH CORE Connectivity Rule 270 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 CAQH CORE Connectivity to create CAQH 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)
Message Transport Layer: *Processing Modes/Interactions*

- CAQH CORE Connectivity Rule addresses both Real time and Batch processing of the payloads and synchronous & asynchronous message interaction patterns
  - Processing Modes describe how message payload is processed

<table>
<thead>
<tr>
<th>Processing Modes Of Payload</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real time</td>
<td>• Entity sends single request, receives single response in real time</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Message Interaction Patterns</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
CAQH CORE Connectivity Rule 270: Error (Acknowledgment) 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
CAQH CORE Connectivity Rule: Security Across the Layers

- Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over common medium of access
- CAQH CORE Connectivity Rule and associated Security Requirements
  - 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
    - CAQH 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

Note: (1) Payload level signature/encryption was evaluated and deferred to date; revisiting in 2012
(2) CORE Connectivity Rules are a base and not a ceiling.
# Federally Mandated CAQH CORE Connectivity Rules: Overview of High-Level Rule Requirements

<table>
<thead>
<tr>
<th>CAQH CORE Connectivity Rule Area</th>
<th>CAQH CORE Rule 153 (Phase I)</th>
<th>CAQH CORE Rule 270 (Phase II)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Internet</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>Transport Security</td>
<td>SSL</td>
<td>SSL, TLS (optional)</td>
</tr>
<tr>
<td>Submitter (Originating System or Client) Authentication</td>
<td>Name/Password</td>
<td>Name/Password X.509 Certificate (subject to conformance requirements)</td>
</tr>
<tr>
<td>Envelope and Attachment Standards</td>
<td>Unspecified</td>
<td>SOAP 1.2 + WSDL and MTOM (for Batch) or HTTP+MIME (subject to conformance requirements)</td>
</tr>
<tr>
<td>Envelope Metadata</td>
<td>Unspecified</td>
<td>Metadata defined (Field names, values) New PayloadTypes for HIPAA and non-HIPAA Payloads</td>
</tr>
<tr>
<td>Message Interactions/ Routing</td>
<td>Real time</td>
<td>Real time</td>
</tr>
<tr>
<td>Acknowledgements, Errors</td>
<td>Specified</td>
<td>Enhanced Phase I, additional specificity on error codes</td>
</tr>
<tr>
<td>Basic Conformance Requirements</td>
<td>Minimally specified</td>
<td>Well specified</td>
</tr>
<tr>
<td>Response Time</td>
<td>Specified</td>
<td>Same as Phase I</td>
</tr>
<tr>
<td>System Availability</td>
<td>Specified</td>
<td>Same as Phase I</td>
</tr>
<tr>
<td>Companion Implementation Guide</td>
<td>Specified</td>
<td>Enhanced Phase I, additional specificity</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules: Message Envelope Standards

- CAQH CORE Connectivity Rule 270 supports two envelope standards (subject to basic conformance requirements)
  - CAQH CORE Connectivity Rule 270 selected HTTP MIME Multipart and SOAP + WSDL as the two standards that met the majority of CORE technical criteria and had wide industry use
  - CAQH CORE Connectivity Rule 270 specifies a SOAP envelope structure using XSD schemas and HTTP MIME envelope using examples

**Envelope Standard A: HTTP MIME Multipart**
- Multipart envelope that is based on MIME standard (non-XML)
- MIME structure supports sending CAQH CORE Connectivity Rule metadata and payload
- Does not provide schemas for envelope

**Envelope Standard B: SOAP 1.2**
- SOAP+WSDL messaging
- Structured envelope that contains CAQH CORE Connectivity Rule metadata and Payload (e.g., using MTOM)
- WSDL and XSD(schema) files are provided files that allow for automated verification
Federally Mandated CAQH CORE Connectivity Rules: 
Payload Processing Modes

- Real Time Payload Processing Requirements:
  - CAQH CORE Connectivity Rule requires Real time (synchronous) processing for X12 v5010 270/271 and X12 v5010 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)
Federally Mandated CAQH CORE Connectivity Rules:
Payload Processing Modes cont’d

• Batch Payload Processing Requirements:
  – Batch (asynchronous) processing is optional for X12 v5010 270/271 and X12 v5010 276/277 transactions
  – **However**, if an entity performs batch processing for X12 v5010 270/271 and X12 v5010 276/277, it must conform to the batch processing specifications for X12 v5010 270/271 and X12 v5010 276/277 transactions in CAQH CORE Connectivity Rule 270 and all other CAQH CORE Mandated Operating Rules.
  – There are a few defined interactions for batch processing within CAQH CORE Connectivity Rule 270:
    • 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
Federally Mandated CAQH CORE Connectivity Rules: *Stakeholder Conformance Guidelines*

- CAQH CORE Connectivity Rules apply 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)

<table>
<thead>
<tr>
<th>If your organization is a:</th>
<th>then your minimum technical role is a:</th>
<th>and CAQH CORE defines technical requirements for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Provider</td>
<td>Client</td>
<td>Client Conformance Requirements</td>
</tr>
<tr>
<td>Clearinghouse/Switch</td>
<td>Client or Server</td>
<td>Client Conformance Requirements</td>
</tr>
<tr>
<td>Health Plan</td>
<td>Server</td>
<td>Server Conformance Requirements</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules: 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.

If your organization is a:

- Health Plan or Clearinghouse/Switch: Then you must implement both of these envelope standards.
- Healthcare Provider: Then implement one of these envelope standards.
Federally Mandated CAQH CORE Connectivity Rules:
Submitter Authentication

- CAQH CORE Connectivity Rules support 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

If your organization is a:

<table>
<thead>
<tr>
<th>Server Conformance Requirements</th>
<th>Health Plan</th>
<th>X. 509 Certificate over SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>then implement one of these authentication standards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Conformance Requirements</th>
<th>Clearinghouse/Switch</th>
<th>Healthcare Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>then you must implement both of these authentication standards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username/Password</th>
<th>X. 509 Certificate over SSL</th>
</tr>
</thead>
</table>
CAQH CORE Envelope Standard B (SOAP+WSDL): Example

- Normative CORE Metadata in Use for SOAP Request (same metadata is used in MIME envelope)

HTTP Headers

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

SOAP Envelope with remaining metadata from CAQH CORE Rule 270

```xml
<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-secesxt-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:PasswordType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-password-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>f61d4fae-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*0000000031]]></Payload>
    </ns1:COREEnvelopeRealTimeRequest>
  </soapenv:Body>
</soapenv:Envelope>
```
CAQH CORE Change Request Process

**Change Request Received**

Types of Requests, e.g.,
- Clarification of rule requirements
- Suggestions for new requirements to address additional transactions, data content, infrastructure, etc.; request to remove or change requirements
- Notice of typographical/grammatical errors
- Analyze possible conflict with standard / question on standard

Source of Requests, e.g.,
- CORE Request Process: CORE@caqh.org
- Entities completing voluntary CORE Certification
- CORE Participant discussions

**CAQH CORE Evaluation of Request**

Substantive/Major Change
(e.g., Changes to rule requirements or new rule ideas)

Alignment with Federal Efforts
(e.g., new versions of standards – v5010)

Non-substantive/Minor Change
(e.g., Typographical/grammatical errors, clarifications or new FAQ)

Review of proposed modification through formal CAQH CORE Rules Development Process

CORE Voting Membership Ballot:
- Requires 60% of membership for quorum
- Two-thirds (66.67%) must vote to approve

Review of proposed modification through with relevant entities (e.g., CMS, ASC X12, NACHA);
modifications made available on CAQH CORE website

Review of proposed modification by CAQH CORE staff and adjustment made if appropriate
Summary

• **CAQH CORE Connectivity Rules**
  – Are being widely implemented to comply with ACA Section 1104
    • HIPAA covered entities like Health Plans, Medicare and State Medicaids need to comply with ACA Section 1104
    • Implementation deadline for HIPAA covered entities is January 1, 2013
  – Have been incorporated into NwHIN X12 Document Submission Specification and esMD Phase I X12 Profile
  – Is well aligned with NwHIN and is payload agnostic, can be used to transport X12 and other payload types

• S&I / esMD can leverage the Federally mandated adoption of CAQH CORE Connectivity Rule base to support shared missions and visions
CAQH CORE Connectivity Rule Implementation: Resources

• **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
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