Overview

- **Purpose**
  - This presentation will provide technical details and review the requirements for implementing the federally mandated CAQH CORE Operating Rules with a focus on those rules related to connectivity.

- **Audience**
  - The intended audience consists of technical implementers of CAQH CORE Connectivity Rules for Eligibility and Claim Status Transactions in your organization.

- **Prerequisites**
  - Basic understanding of CAQH CORE mission, vision and Guiding Principles; please 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 Message Envelope Protocols including SOAP+WSDL or HTTP+MIME multipart.

- **Required Materials**
  - This PowerPoint and a copy of the CAQH CORE Connectivity Operating Rules for reference.
  - Phase I Connectivity click HERE.
  - Phase II Connectivity click HERE.

Presentation Outline

- **Technical Concepts: Mandated CAQH CORE Connectivity Operating Rules**
  - Safe Harbor Principle
  - Message Envelope Standards
  - Payload Processing Modes and Messaging Interaction Types

- **Technical Requirements: Mandated CAQH CORE Connectivity Operating Rules**
  - Envelope Requirements
  - Security Requirements
  - Payload Processing Mode Requirements
  - Conformance Requirements for Stakeholders
  - Requirements based on other CAQH CORE Infrastructure Operating Rules

- **Q&A/Commonly Asked Questions**

- **CAQH CORE Resources for Implementers**
**Federally Mandated CAQH CORE Connectivity Rules:**

The focus of the presentation is on Connectivity Rules.

<table>
<thead>
<tr>
<th>Rule Types</th>
<th>Transactions</th>
<th>Rule Areas</th>
<th>CAQH CORE Rule Numbers</th>
<th>Key Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>X12 270/271 Eligibility &amp; Benefits</td>
<td>Response Time Rules: (Batch &amp; Real Time) &amp; System Availability Rules</td>
<td>155, 156, 157, 158</td>
<td>Compatibility of the CAQH CORE Infrastructure Rules must be considered during implementation.</td>
</tr>
<tr>
<td></td>
<td>X12 276/277 Claims Status</td>
<td>Connectivity Rules</td>
<td>156</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Companion Guide Rule</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Data Content</td>
<td>X12 270/271 Eligibility &amp; Benefits</td>
<td>Normalizing Patient Last Name &amp; AAA Code Reporting Rules</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>155</td>
<td>Data Content Rules apply only to the Eligibility &amp; Benefit transaction.</td>
</tr>
</tbody>
</table>

*CAQH CORE Rule 250 applies the CAQH CORE Infrastructure Rules to the X12 276/277 Claims Status transaction.*

**Federally Mandated CAQH CORE Connectivity Rules**

- **Problem addressed by rules**
  - Multiple methods for exchanging eligibility and benefits data both manually and/or electronically drive elevated transaction costs and increase operational complexity.

- **Scope of the rules**
  - Using the internet as a delivery option, establishes a “Safe Harbor” connectivity rule which standardizes the flow of administrative transactions between health plan and provider.
    - Rule 270 builds on Rule 153 to include more prescriptive submitter authentication, envelope specifications, etc.
    - Safe Harbor applies when an entity uses, conducts or processes the X12 270/271 Eligibility & Benefits and X12 276/277 Claim Status 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.

**Federally Mandated CAQH CORE Infrastructure Rules**

- **Connectivity Rules**
  - Clients and servers must follow requirements in the CAQH CORE Connectivity Rules: CAQH CORE Rules 270 and 153.

- **Response Time Rules**
  - Servers must follow the requirements for response times for Real time interactions in CAQH CORE Real time Response Time Rule: CAQH CORE Rule 156.
  - Servers must follow the requirements for response times for Batch interactions as stated in CAQH CORE Batch Response Rule: CAQH CORE Rule 155.

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

- **Companion Guide Requirement**
  - Servers must publish detailed specifications in a Connectivity Companion Guide; the guide should be consistent with the guidelines for companion guides described in the CAQH CORE Connectivity Rule 270.
  - CAQH CORE makes recommendations in CAQH CORE Connectivity Rule 270 for specific topics and information in the Companion Guide.

*NOTE: Many of the Federally mandated CAQH CORE Infrastructure Rules also apply to the ASC X12 v5010 835 per CMS-0028-IFC.*
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 are a set of requirements that represent a minimum level of requirements
  - Entities may go above and beyond the rules to ensure the implementations meet their needs

Federally Mandated CAQH CORE Connectivity Rules:

Connected Systems and Applicable Architectures

- Interoperability and efficiency is enhanced by the rules defined technical requirements for exchange of administrative transactions between trading partners
  - Connectivity Rules can be applied independent of the communication architecture or model (e.g., two models are shown below)
  - Connectivity Rules do not apply to Direct Data Entry (DDE) systems

Federally Mandated CAQH CORE Connectivity Rules:

Message Interactions

- CAQH CORE Connectivity Rules apply to the message interactions between connected systems
  - CAQH CORE Connectivity Rules are a set of operating rules that describe on an operational level how the systems should interact
  - The rules contain details that include the message format, the response times, authentication methods, and responsibilities based on roles of the senders and receivers
  - CAQH CORE Connectivity Rules set a minimum level of security, designed to protect the information and communication channels; entities may implement additional security measures
Federally Mandated CAQH CORE Connectivity Rules:

Security

The security aspects of CAQH CORE Connectivity Rules are intended to ensure:

- A message is not tampered with while traveling to partner systems
- The message came from a known partner

Description of CAQH CORE Connectivity Rules with Direct (i.e., with no intermediaries) Connectivity Example

Messages are protected while traveling to destination

Provider (Client)  Health Plan (Server)

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

Federally Mandated CAQH CORE Connectivity Rules:

Layered View

Application Layer:
- CAQH CORE Connectivity Rules are "Payload Agnostic", hence do not specify the Application file or processing layer

Message Encapsulation Layer:
- CAQH CORE Connectivity Rules define a prescriptive Message Envelope structure and metadata

Message Transport Layer:
- Both CAQH CORE Connectivity Rules 153 and 270 prescribe use of a securely encrypted Message Transport Layer
- Both require HTTP over SSL; CAQH CORE Rule 270 includes optional use of TLS

Federally Mandated CAQH CORE Connectivity Rules:

Safe Harbor Principle

The connectivity requirements that a trading partner must use if requested by another trading partner are described in the CAQH CORE Connectivity Rules as the CORE Connectivity Safe Harbor

CAQH CORE Rule 270, Section 5, CORE Safe Harbor, defines the CAQH CORE Connectivity Safe Harbor

- The CAQH CORE Connectivity 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 trading partner to exchange data using the CAQH CORE Connectivity Rule

- The rule does not require entities to remove existing connections that do not match the rule. Nor does it require that all covered entities use this method for all new connections. In some circumstances, you and your trading partners may decide to continue to use your current connection; however you must implement the capability to use the CORE Connectivity Safe Harbor when requested.
Federally Mandated CAQH CORE Connectivity Rules:
Message Envelope Standards

- CAQH CORE Connectivity Rules support 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 CAQH 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/Interactions

- CAQH CORE Connectivity Rules address both Real time & Batch payload processing modes
- Payload Processing Modes describe how message payload is processed

<table>
<thead>
<tr>
<th>Processing Modes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Real time        | - Entity sends single request, receives single response in Real time
                  | - Servers must follow the requirements for response times for Real time interactions in CAQH CORE Real time Response Rule: CORE Rule 156 |
| Batch            | - Entity submits Batch of requests at the same time
                  | - Message of processing the Batch of requests are sent back at a later time (i.e., not in Real time)
                  | - Batch (asynchronous) processing is optional for X12 v5010 270/271 and X12 v5010 276/277 transactions |

Federally Mandated CAQH CORE Connectivity Rules:
Payload Processing Modes and Messaging Interactions

CAQH CORE Connectivity Rule 270 addresses synchronous & asynchronous message interaction pattern: 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

Real time request and response occur in the same connection session

Batch request and response occur in different connection sessions
Are You Ready for Trading Partner Testing?

- Testing with your trading partners is a critical aspect to making your operating rules implementation a success, as well as that of those entities with which you exchange HIPAA transactions.
- Given the Federal deadline for the 1st set of operating rules is January 1, 2013, CAQH CORE is now hosting a website to highlight those organizations in trading partner testing.
- HIPAA covered entities (or other key IT systems that support them, such as Practice Management Systems) can quickly list that their organization is ready to test with its trading partners.
  - Those entities using the website that are voluntarily CORE-certified have their CORE Certification Seal listed, given such entities already are using the CORE rules in daily exchange and thus able to test with their trading partners.
- The website can be found at http://caqh.org/COREPartnerTesting.php.

If you are ready, add your organization today!

Technical Requirements of Mandated CAQH CORE Connectivity Operating Rules

<table>
<thead>
<tr>
<th>CAQH CORE Connectivity Rule Area</th>
<th>CAQH CORE Connectivity Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Internet</td>
</tr>
<tr>
<td>Transport</td>
<td>HTTP</td>
</tr>
<tr>
<td>Transport Security</td>
<td>SSL, TLS optional</td>
</tr>
<tr>
<td>Submitter (Originating System or Client) Authentication</td>
<td>X.509 Certificate (subject to conformance requirements)</td>
</tr>
<tr>
<td>Envelope and Attachment Standards</td>
<td>SOAP 1.2 or WSDL for exchange of HIPAA and non-HIPA (optional)</td>
</tr>
<tr>
<td>Envelope Metadata</td>
<td>Metadata defined if first names, values</td>
</tr>
<tr>
<td>Message Interactions</td>
<td>Real-time, Reliable, Reliable, Reliable</td>
</tr>
<tr>
<td>Routing</td>
<td>Real/Reliable/Reliable/Reliable</td>
</tr>
<tr>
<td>Error Acknowledgments, Errors</td>
<td>Specified</td>
</tr>
<tr>
<td>Dead-End Conformance Requirements</td>
<td>Specified</td>
</tr>
<tr>
<td>Message Integrity</td>
<td>Specified</td>
</tr>
<tr>
<td>System Availability</td>
<td>Specified</td>
</tr>
<tr>
<td>Companion Implementation Guide</td>
<td>Specified</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rules:

**Message Structure**

- CAQH CORE Connectivity Rule 270 metadata is prescriptive to facilitate interoperability of administrative transactions

- Public Internet (TCP/IP) – CORE Connectivity Rule 153
- HTTP over SSL (HTTP/S) – CORE Connectivity Rule 153 (includes security of payload during transmission)
- Message Envelope & Message Metadata – CORE Connectivity Rule 270 Rule (independent of payload – required by CORE Connectivity Rule 153)
- HIPAA Administrative Transactions (X12)
- NLT Clinical Messages
- Zipped Files
- Personal Health Record
- Other Content

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

For reliability of transport:
- UUID is used for Payload ID (for detecting duplicates)
- Timestamp is used for ensuring that the data is recent

For payload integrity verification:
- Hash (e.g., SHA-1 Checksum of the payload) is sent as part of the message envelope

For payload encryption:
- SSL (3.0 and optionally TLS) for transport level security
- Servers are authenticated using SSL Server Certificates
- SHA-1 Algorithm is used for message payload
- Username and Password (e.g., WS-Profile)

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

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

- CAQH CORE Connectivity Rules’ 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 version
  - Servers are authenticated using SSL Server Certificates
  - 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 is used for Payload ID (for detecting duplicates)
    - Timestamp is used for ensuring that the data is recent

Note: CAQH CORE Connectivity Rules are a base, not a ceiling
Federally Mandated CAQH CORE Connectivity Rules: Payload Processing Modes

- **Real time Payload Processing Requirements:**
  - 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 con conform to the batch processing specifications for X12 v5010 270/271 and X12 v5010 276/277 transactions
  - 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: Error Handling

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status and Error Codes</td>
<td>Returned the IETF RFC 2616 for the specific and complete list of protocol specific errors that must be supported.</td>
</tr>
<tr>
<td>CAQH CORE Connectivity Rules (270 and 271)</td>
<td>Describe transport level status and error conditions and the use of HTTP status and error codes for those conditions.</td>
</tr>
<tr>
<td>Envelope Processing Status and Error Codes</td>
<td>Errors while processing the envelope (e.g., rule version mismatch). Error codes are enumerated as CAQH CORE Connectivity Rule 270.</td>
</tr>
<tr>
<td>Payload Processing Error Messages</td>
<td>Returned processing status (e.g., ASC X12 TA1) or errors (e.g., ASC X12 TA5) are the responsibility of the application. (The HHS Final Rule for Administrative Simplification Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transaction does not require compliance with any operating rule requirements related to acknowledgments, the Final Rule does note “we are addressing the important role that acknowledgments play in EDI by strongly encouraging the industry to implement the acknowledgement requirements in the CAQH CORE rules we are adopting herein.”)</td>
</tr>
</tbody>
</table>

---
Federally Mandated CAQH CORE Connectivity Rules:

**Error Handling**

- Once request (e.g., X12 270) is submitted, it goes through 3 logical layers:
  - Processing of HTTP headers (typically handled by a web server)
  - Processing the Envelope (can be handled by messaging middleware or integration brokers)
  - Processing the Payload (e.g., ASC X12, typically handled by application business logic)
- At each layer, some part of the request is processed and errors can be returned to the 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 Processing Layer, it returns a response or error

---

**Stakeholder Conformance Guidelines**

- CAQH CORE Connectivity Rules apply to health plans (HTTP/S server) and health care providers (HTTP/S client)
  - The 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)

---

**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
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

Then you must implement both of these authentication standards

Username/Password

X.509 Certificate over SSL

30-Minute Q & A:
Technical Questions on Mandated CAQH CORE Connectivity Rules

Your feedback will help us with new CAQH CORE reference materials

Federally Mandated CAQH CORE Connectivity Rules:
Frequently Asked Questions

Questions
1. Real time. Is this required? Can you tell me definitively? Do we have to implement real time even if none of our trading partners are asking for it?
2. Do we have to implement or can we offer Batch over our FTP?
3. If a health plan only accepts transactions from its clearinghouse, must the health plan also implement CAQH CORE connectivity, or can the health plan delegate that responsibility to the clearinghouse?
4. How is downtime defined/measured?
5. How is the 20 second response time measured?
6. What data do I have to track/audit? Do I have to deliver this data to anyone?
7. What are the minimum interactions that must be supported for compliance with the CAQH CORE 270 Connectivity Rule?
8. How does the CORE Companion Guide Rules 152 and 250, which require the use of the CAQH CORE Master Companion Guide Template, relate to the CORE Connectivity Rule which requires a Server-Specific Connectivity Guide?

OTHER
1. Please submit your questions during this presentation to the Q&A
2. After the presentation submit your questions to CORE@caqh.org