Committee on Operating Rules For Information Exchange (CORE®)

Phase IV CORE Connectivity, Security, and Related Infrastructure

December 5, 2013
Discussion Topics

• Recap: CAQH CORE Connectivity Background

• Recap: Federally Mandated CAQH CORE Connectivity Rule v2.2.0

• Preliminary Business and Market Analysis to Consider when Evaluating Phase IV CAQH CORE Connectivity Opportunities
  – CAQH CORE Criteria: Business and Technical
  – Industry Trends:
    • Private/Government Initiatives with emphasis on reviewing DIRECT
    • Connectivity Technical Trends

Appendix

*Also known as CAQH CORE 270: Connectivity Rule (v2.2.0)
Recap:

CAQH CORE Connectivity and Security Background
CAQH CORE Mission

To build consensus among the essential healthcare industry stakeholders on a set of operating rules that facilitate administrative interoperability between health plans and providers

• Support applicable HIPAA transaction requirements
• Enable providers to submit transactions from any system
• Enable stakeholders to implement CAQH CORE in phases
• Facilitate stakeholder commitment to and compliance with CAQH CORE
• Facilitate administrative and clinical data integration

Key things CAQH CORE will not do:

• Build a database
• Replicate Federally adopted standards from bodies like W3C, OASIS, X12 or HL7
CAQH CORE Guiding Principles

• CAQH CORE will not create or promote proprietary approaches to electronic interactions/transactions.

• Whenever possible, CAQH CORE has used existing market research and proven rules. CAQH CORE Rules reflect lessons learned from other organizations that have addressed similar issues.

• CAQH CORE will suggest migration steps to promote successful and timely adoption of CAQH CORE Rules.

• All CAQH CORE recommendations and rules will be vendor neutral.

• Rules will not be based on the least common denominator but rather will encourage feasible progress, promote cost savings, and efficiency.

• To promote interoperability, rules will be built upon HIPAA, and align with other key industry bodies.

• Where appropriate, CAQH CORE will address the emerging interest in XML, or other evolving standards.

• CAQH CORE Rules will support the Guiding Principles of HHS’s National Health Information Network (NwHIN).

• CAQH CORE will not build a switch, database, or central repository of information.

• CAQH CORE participants do not support “phishing.”

• CAQH CORE Rules address both batch and real time, with a movement towards real time (where/when appropriate).

• All of the CAQH CORE Rules are expected to evolve in future phases.
CAQH CORE Guiding Principles Specific to Connectivity

• Developed using consensus-based, multi-stakeholder approach and is designed to:
  – Facilitate interoperability
  – Improve utilization of electronic transactions
  – Enhance efficiency and help lower the cost of information exchange in healthcare
  – Support a range of administrative transactions

• Builds upon existing standards

• Focused on Business to Business (B2B) transactions

• Creates a base and not a “ceiling”
  – E.g., CORE-certified entities need to provide CORE-certified connectivity interface but may offer additional connectivity interfaces to support their business needs

• Provides a “safe harbor”
  – Rule is supported/offered by any CORE-certified entity

• Connectivity Rules do not:
  – Require trading partners to remove existing connections that do not match the rule
  – Require that all CORE-certified entities use the CAQH CORE Rule for all new connections
Subgroup Charge and Responsibilities

• Support adherence to the CAQH CORE mission through the development of a phase-specific CAQH CORE Connectivity and Security Rule and related infrastructure rules

• If not already, become familiar with the Phase I and Phase II CAQH CORE Connectivity Rules: Phase I CAQH CORE Connectivity Rule; Phase II CAQH CORE Connectivity Rule
  – The existing CAQH CORE Operating Rules are already mandated; future versions may update/replace earlier versions, however, entities must still meet existing mandates, e.g., January 2014 EFT/ERA

• If you have completed Phase I or Phase II implementation, share your experiences
  – If you are not the person responsible for connectivity in your organization, identify and reach out to the appropriate person so that your organization’s implementation of this and other connectivity methods is part of the Subgroup discussion

• Attend and be active on Subgroup calls – will be meeting from now until Q2/Q3 2014
  – Read materials before calls whenever possible
  – Review materials after the calls and be prepared to participate in sharing feedback via straw polls, etc.

• If you determine you are not the appropriate subject matter expert (SME) in this area, reach out to your CORE representative so he/she can identify the SME

• Understand the quorum and implementer–focused CORE voting process (see appendix)

• Remember the focus is on the system at-large
Attributes of Subgroup Participants

Attendees should have:

• Knowledge of the definition and scope of operating rules per the ACA and background on the already Federally-mandated operating rules (eligibility, claim status, EFT/ERA)

• Understanding of foundational principles and concepts for the mandated CAQH CORE Connectivity Rule for the eligibility, claim status, and EFT/ERA transactions

• Ideas and open minds on how connectivity/security/infrastructure operating rules can improve and support the Phase IV CAQH CORE Operating Rules by transaction (claims, prior authorization, premium payments, disenrollment/enrollment, and attachments; noting attachments standards are not yet mandated but connectivity will need to support capacity to send large volumes of electronic documents)

• Knowledge of larger industry and alignment with Federal HIT initiatives

• Ability and preparedness to participate in CAQH CORE Connectivity industry surveys

• Basic understanding of technical concepts like:
  – Networking concepts and basics used for client/server and server to server connectivity
  – Message Envelope Protocols like SOAP or MIME messaging
  – Security concepts like SSL and TLS
  – Knowledge of organization’s current messaging systems
General CORE Connectivity Criteria Applicable to Phase IV

**General Principles**

- Supports large batch transaction files
- Supports real time payload (transaction) processing
- Supports large volume of single real time transaction processing
- Has extensive message attributes
- Supports Synchronous (i.e., request/response on single connection) and Asynchronous (i.e., response initiated by responder on separate connection) message exchanges
- Supports point-to-point message exchanges
- Supports push and pull messaging
- Supports rules based routing

**Reliable Messaging**

- Payload independence
- Message metadata

**Implementation Business Principles**

- Language neutral
- Platform neutral

**Interoperability Principles**

- Compatible with emerging clinical standards for interoperability

**Security Principles**

- Supports submitter (initializing system or client) authentication
- Supports encrypted authentication
- Supports digital certificates
Phase IV CAQH CORE Connectivity Rule

Process Overview

1. Phase IV Requirements Selection

2. Environmental Scan

3. Evaluation of Criteria

4. Tech-Functional Capabilities/Selected Requirements/Standards Overlay
   - Do one or more standards satisfy the criteria?

5. Select standard(s) for Connectivity Rule

6. Specify Rule
Phase IV CAQH CORE Connectivity Rule

Proposed Rule Development Approach & Timeline

Subgroup will meet from now through Q2/Q3 2014 and will begin updating Work Group when criteria are finalized. Any rule drafted by Subgroup must have Work Group approval and all-CORE approval (which is implementer focused).
Recap: Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Federally Mandated CAQH CORE Connectivity Rule v2.2.0

Problem Addressed & Scope

• **Problem addressed by rule**
  
  – Multiple methods for exchanging administrative transaction data both manually and/or electronically drive elevated transaction costs and increase operational complexity

• **Scope of the rule**
  
  – 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 or “B2B”
  
  – 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 Operating Rules

Notes:
1) Data content rules can apply to all transactions addressed by CAQH CORE Operating Rules.
2) CAQH CORE Connectivity Rule and other infrastructure rules currently apply to all operating rules with the exception of EFT which uses a different infrastructure/connectivity (ACH network).
3) Safe Harbor principle applies only to CAQH CORE Connectivity Rule. Connectivity approaches outside Safe Harbor still need to comply with all other rule requirements (infrastructure and content).
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Connected Systems and Applicable Architectures

- Interoperability and efficiency is enhanced by the rule’s defined technical requirements for exchange of administrative transactions between trading partners, also known as a Business to Business (B2B) relationship
  - Connectivity Rule can be applied independent of the communication architecture or model (e.g., two models are shown below)
  - Connectivity Rule does not apply to Direct Data Entry (DDE) systems

**Model 1: B2B Connectivity**

![Diagram of B2B Connectivity]

Provider ➔ Health Plan

**Not Applicable: B2C Connectivity**

![Diagram of B2C Connectivity]

Business ➔ Consumer

**Model 2: B2B Connectivity with Intermediary**

![Diagram of B2B Connectivity with Intermediary]

Provider ➔ Clearinghouse ➔ Health Plan
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
High-Level Rule Requirements

<table>
<thead>
<tr>
<th>Connectivity Rule Area</th>
<th>Rule Requirements</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>Name/Password&lt;br&gt;X.509 Certificate (subject to conformance requirements)</td>
</tr>
<tr>
<td>Envelope and Attachment Standards</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>Metadata defined (field names, values)&lt;br&gt;New PayloadTypes for HIPAA and non-HIPAA Payloads</td>
</tr>
<tr>
<td>Message Interactions/ Routing</td>
<td>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)</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Specifies error codes that must be returned for error conditions</td>
</tr>
<tr>
<td>Basic Conformance Requirements</td>
<td>Specifies for information sources performing role of HTTP/S server and information receivers performing role of HTTP/S client</td>
</tr>
<tr>
<td>Response Time</td>
<td>Real time: Maximum response time from time of submission must be 20 seconds (or less)&lt;br&gt;Batch: Response to transaction submitted by 9:00 pm E.T. must be returned by 7:00 am E.T. following business day</td>
</tr>
<tr>
<td>Companion Implementation Guide</td>
<td>Specific requirements for publication of entity-specific connectivity companion guide</td>
</tr>
</tbody>
</table>
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Layered View

**Application Layer:**
- CAQH CORE Connectivity Rule is “Payload Agnostic”, hence do not specify the Application file or processing layer

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

**Message Transport Layer:**
- Both CAQH CORE Connectivity Rules prescribe use of a securely encrypted Message Transport Layer
  - Both require HTTP over SSL
  - Optional use of TLS 1.0
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Security Across the Layers

- Transport Security: Security (e.g., authentication, integrity) for electronic transactions conducted over common medium of access
- CAQH CORE Connectivity Rule v2.2.0 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
    - 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 Rule is a base, not a ceiling
* SHA-1 requirements: http://tools.ietf.org/html/rfc3174
Preliminary Business and Market Analysis: Criteria
Industry Landscape
Legislative, Market Movements and National Initiatives

Legislative and National Initiatives Movement towards increased adoption of Standards

**Legislative Movement**
- HIPAA covered entities are implementing CAQH CORE Connectivity for ACA Section 1104 compliance
- Meaningful Use Stage 2 has transport requirements for Providers/EHR systems such as use of ONC DIRECT
- HITECH Act has greater security requirements, penalties for lack of security

**Interoperability Initiatives**
- CAQH CORE
- eHealth Exchange (formerly NwHIN)
- ONC S&I esMD has adopted CAQH CORE Connectivity
- Trust policy frameworks developed by DirectTrust, white papers by ONC S&I esMD Author of Record

**Market Movement towards increased Connectivity, new Business Needs**

**Market Movement**
- Market movement from paper based to Internet based electronic transactions.
- Efficiencies of scale gained as more trading partners support electronic transactions
- Improved efficiency as more electronic transactions become standards based

**Technical Impact of Direct Connectivity**
- Need to support standards in new areas such as attachments
- Need for reliability and security in support of the new business transactions

**Government PKI Infrastructures**
- Federal Bridge is built and operational supporting cross-certification of trusted PKIs
Phase IV CAQH CORE Connectivity
Rationale for Business and Technical Criteria Selection

- Advances administrative simplification and efficiency and larger mission goals
  - Recent CAQH CORE infrastructure survey of industry participants (over 130 organizations) indicated strong interest (over 80% for all transactions in Phase IV) in the continued application of CAQH CORE Connectivity Rule v2.2.0 to the next set of ACA mandated transactions
  - There were some comments that, for certain transactions only, batch connectivity and associated infrastructure should be considered

- Meets the scope and requirements needs of regulations
  - Example: Operating rules cannot directly apply to Employers or PMS

- Conforms to established CAQH CORE Guiding Principles, CAQH CORE Connectivity Guiding Principles, and Connectivity Technical Criteria (see following slides)

- Leverages existing CAQH CORE install base and implementer experience
  - Voluntary CORE Certification process will be leveraged for testing technical conformance
  - CORE Certification Test Suite will be built for each CAQH CORE Operating Rule, including next CAQH CORE Connectivity Rule

- Leverages work done by other major initiatives with national scope
  - Major initiative will have national scope and have a current nationwide implementation base or have a path to nationwide implementation through regulatory adoption, e.g. ONC DIRECT
# Phase IV CAQH CORE Connectivity

## Established Business Criteria

<table>
<thead>
<tr>
<th>CAQH CORE Guiding Principles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CAQH CORE will not create or promote proprietary approaches to electronic interactions/transactions</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE Rules reflect lessons learned from other organizations that have addressed similar issues</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE will suggest migration steps to promote successful and timely adoption of CAQH CORE Rules</td>
<td></td>
</tr>
<tr>
<td>• All CAQH CORE recommendations and rules will be vendor neutral</td>
<td></td>
</tr>
<tr>
<td>• Rules will not be based on the least common denominator but rather will encourage feasible progress, promote cost savings, and efficiency</td>
<td></td>
</tr>
<tr>
<td>• To promote interoperability, rules will be built upon HIPAA, and align with other key industry bodies</td>
<td></td>
</tr>
<tr>
<td>• Where appropriate, CAQH CORE will address the emerging interest in XML, or other evolving standards</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE Rules will support the Guiding Principles of HHS’s National Health Information Network</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE will not build a switch, database, or central repository of information</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE Participants do not support “phishing”</td>
<td></td>
</tr>
<tr>
<td>• CAQH CORE Rules address both batch and real time, with a movement towards real time (where/when appropriate)</td>
<td></td>
</tr>
<tr>
<td>• All of the CAQH CORE Rules are expected to evolve in future phases.</td>
<td></td>
</tr>
<tr>
<td>• Developed using consensus-based, multi-stakeholder approach</td>
<td></td>
</tr>
<tr>
<td>• Builds upon existing standards</td>
<td></td>
</tr>
<tr>
<td>• Focused on Business to Business (B2B) transactions</td>
<td></td>
</tr>
<tr>
<td>• Creates a base and not a “ceiling”</td>
<td></td>
</tr>
<tr>
<td>• Provides a “safe harbor”</td>
<td></td>
</tr>
</tbody>
</table>
## Phase IV CAQH CORE Connectivity
### Established General Connectivity Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
</table>
| **General Principles** | • Supports large batch transaction files  
• Supports real time payload (transaction) processing  
• Supports large volume of single real time transaction processing  
• Has extensive message attributes  
• Supports Synchronous (i.e., request/response on single connection) and Asynchronous (i.e., response initiated by responder on separate connection) message exchanges  
• Supports point-to-point message exchanges  
• Supports push and pull messaging  
• Supports rules based routing |
| **Security Principles**| • Supports submitter (initialing system or client) authentication  
• Supports encrypted authentication  
• Supports digital certificates |
| **Reliable Messaging** | • Payload independence  
• Message metadata |
| **Implementation Business Principles** | • Language neutral  
• Platform neutral |
| **Interoperability Principles** | • Compatible with emerging clinical standards for interoperability  
(Subgroup highlighted growing trend for EHR/PMS convergence and thus need to support alignment of EHRs/PMS.) |
<table>
<thead>
<tr>
<th>Business Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost savings through interoperability</td>
<td>Any rule enhancements must be driven by improvements in efficiency and cost savings through better interoperability.</td>
</tr>
<tr>
<td>Criteria for classification as a major initiative</td>
<td>Major initiative will have national scope and have a current nationwide implementation base or have a path to nationwide implementation through regulatory adoption; also, <em>sustainability and overall integration into helping maintain and develop unfunded data exchange requirements</em>.</td>
</tr>
<tr>
<td>CMS regulatory requirement to support transactions and their attachments</td>
<td>ACA Section 1104 mandates next set of operating rules support the following transactions:</td>
</tr>
<tr>
<td></td>
<td>• Health Claims or equivalent encounter information</td>
</tr>
<tr>
<td></td>
<td>• Enrollment and dis-enrollment in a health plan</td>
</tr>
<tr>
<td></td>
<td>• Health plan premium payments</td>
</tr>
<tr>
<td></td>
<td>• Referral certification and authorization</td>
</tr>
<tr>
<td></td>
<td>• Attachments</td>
</tr>
<tr>
<td>CMS timeline for drafting a Phase IV rule set is 2014 and other industry priorities</td>
<td>HHS Secretary has recommended CAQH CORE as the author for these operating rules. The effective date for these rules is January 1, 2016; drafting is somewhat delayed as it HHS certification for initial two sets of operating rules. CAQH CORE will review drafts to NCVHS by Q3 2014 and HHS will determine final rules and deadlines. New features should consider timeline and other industry priorities.</td>
</tr>
<tr>
<td>Alignment with clinical domain's interoperability standards</td>
<td>CAQH CORE has always supported alignment between admin and clinical as a guiding principle. Given there are incentive-based Meaningful Use regulations provider systems must comply with, it would help the industry if MU and ACA are aligned in the area of interoperability and data exchange standards, and improve ROI by reusing technologies and expertise across clinical and admin going forward.</td>
</tr>
<tr>
<td>Align with current major national initiatives</td>
<td>Alignment can be at various levels, such as transport, envelope, security and metadata. The level of alignment will need to be considered carefully.</td>
</tr>
<tr>
<td>New Connectivity Rule should provide sufficient increase in efficiencies and returns on investment (ROI) for the industry</td>
<td>Relative to the investments already made in complying with ACA Section 1104, provide sufficient increase in efficiency and ROI.</td>
</tr>
</tbody>
</table>
## Core Technical Guiding Principles for Connectivity

<table>
<thead>
<tr>
<th>Technical Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed using consensus-based, multi-stakeholder approach</td>
<td></td>
</tr>
<tr>
<td>Builds upon existing standards</td>
<td></td>
</tr>
<tr>
<td>Focused on Business to Business (B2B) transactions</td>
<td></td>
</tr>
<tr>
<td>Creates a base and not a “ceiling”</td>
<td></td>
</tr>
<tr>
<td>Provides a “safe harbor”</td>
<td></td>
</tr>
<tr>
<td>Supports large batch transaction files</td>
<td></td>
</tr>
<tr>
<td>Supports real time transaction processing</td>
<td></td>
</tr>
<tr>
<td>Supports large volume of single real time transaction processing</td>
<td></td>
</tr>
<tr>
<td>Has extensive message attributes</td>
<td></td>
</tr>
<tr>
<td>Supports Synchronous and Asynchronous message exchanges</td>
<td></td>
</tr>
<tr>
<td>Supports point-to-point message exchanges</td>
<td></td>
</tr>
<tr>
<td>Supports push and pull messaging</td>
<td></td>
</tr>
<tr>
<td>Supports rules based routing</td>
<td></td>
</tr>
<tr>
<td>Supports submitter (initialing system or client) authentication</td>
<td></td>
</tr>
<tr>
<td>Supports encrypted authentication</td>
<td></td>
</tr>
<tr>
<td>Supports digital certificates</td>
<td></td>
</tr>
</tbody>
</table>
## Phase IV CAQH CORE Connectivity

### Preliminary Technical Criteria

<table>
<thead>
<tr>
<th>Technical Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support for unstructured attachments, with movement towards structured</strong></td>
<td>As per CAQH CORE and NCVHS testimonies, the first step in migrating the industry from paper based attachments is unstructured attachments with a movement towards structured needs.</td>
</tr>
<tr>
<td><strong>Payload agnostic</strong></td>
<td>Must be independent of the type of payload being transported.</td>
</tr>
<tr>
<td><strong>Support for large attachments</strong></td>
<td>Large attachment handling may impose specific constraints on the transport, envelope and message interaction modes.</td>
</tr>
<tr>
<td><strong>Security of sensitive information in transactions and attachments is preserved</strong></td>
<td>Securing the transactions and attached files through the use of authentication, authorization, integrity, signature, non-repudiation, and delegation of rights</td>
</tr>
<tr>
<td><strong>Plug-and-play interoperability through prescriptive specification with fewer options</strong></td>
<td>CAQH CORE Connectivity Rule v2.2.0 is a highly prescriptive rule, but it has some options (with basic conformance requirements for organizations) in the envelope and authentication standards. Convergence to a single envelope standard and authentication standard was a stated long-term vision in previous phases</td>
</tr>
<tr>
<td><strong>Backward compatibility</strong></td>
<td>Interoperability with existing implementation of CAQH CORE v2.2.0 Connectivity. <strong>Important Note:</strong> Criteria needs to be carefully evaluated against the need to support new features that may be needed for the next set of Operating Rules.</td>
</tr>
</tbody>
</table>
Preliminary Business and Market Analysis:
*Key Connectivity Industry Trends*
Connectivity Environment Scan

Major National Initiatives

The following is a non-exhaustive list of prominent private industry initiatives in healthcare connectivity and security:

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Primary Business Focus Area</th>
<th>Key Features/Differentiators</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAQH CORE Connectivity (Federally mandated for ACA Section 1104)</td>
<td>Administrative Simplification in healthcare transactions between Providers and Payers</td>
<td>• Simplicity, Plug-and-Play interoperability and security</td>
<td>• Real Time &amp; Batch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prescribes transport, envelope, metadata, security</td>
<td>• B2B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Safe Harbor allows other approaches</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Federally mandated as part of Affordable Care Act for Eligibility, Claim Status and ERA transactions</td>
<td></td>
</tr>
<tr>
<td>NCPDP Connectivity Guide (Retail Pharmacy based on CORE Connectivity)</td>
<td>Administrative Simplification in pharmacy transactions between Pharmacies and Payers</td>
<td>• Simplicity, Plug-and-Play interoperability, Security</td>
<td>• Real Time &amp; Batch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prescribes envelope and security but not transport</td>
<td>• B2B</td>
</tr>
<tr>
<td>‡HealtheWay - eHealth Exchange (formerly NwHIN Exchange) (included in Meaningful Use-2)</td>
<td>Operational support for NwHIN Exchange - government projects that use NwHIN Specifications for health data exchange</td>
<td>• Currently being managed by HealtheWay, a private entity</td>
<td>• Real Time &amp; Batch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Based on NwHIN Specifications developed by HHS ONC, with the primary focus area of clinical data exchange</td>
<td>• B2B</td>
</tr>
<tr>
<td>Health Level 7 (HL7)</td>
<td>Clinical structured and un-structured data and associated security</td>
<td>• This is a data content standard for clinical information</td>
<td>Not a connectivity standard</td>
</tr>
<tr>
<td>DirectTrust</td>
<td>Created by and for participants in the Direct community. Goal being to establish and maintain a national Security and Trust Framework in support of Direct exchange.</td>
<td>• Creates policy and certification requirements for participants within the Direct environment.</td>
<td>• Connectivity Security Policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distributes Trust Bundles</td>
<td>• B2B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• B2C</td>
</tr>
</tbody>
</table>

‡ HealtheWay is a private company sponsored to provide operational support for government/ONC projects.
The following is a non-exhaustive list of prominent government-led initiatives in healthcare connectivity and security:

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Primary Business Focus Area</th>
<th>Key Features/Differentiators</th>
<th>Applicability</th>
</tr>
</thead>
</table>
| ONC DIRECT (included in Meaningful Use-2) | Clinical document sending (push) between Providers | • Direct transport access to both large and small providers  
• Simplicity and security with low entry barrier  
• Adopted into Meaningful Use Stage 2 requirements for EHR Systems | • Batch (one-way push)  
• B2C  
• B2B |
| ONC S&I Electronic Submission of Medical Documents (esMD) and Electronic Determination of Coverage (eDoc) | Support for document submission towards fraud and abuse countering support in the Adjudication of Electronic Claims. The scope is evolving to include and Determination of Coverage and the associated document submissions. | • Use of CAQH CORE Connectivity as transport option for commercial payers.  
• Use of ONC Direct as a transport option for commercial payers.  
• Use of NwHIN X12 Document Submission (combination of CORE Connectivity with added security requirements) for CMS Medicare | • Batch (with movement towards real time)  
• B2B |
ONC DIRECT: Background and Rationale for CAQH CORE Review

High Level Background

- Direct is a clinical data exchange specification developed under the leadership of ONC
- Secure email based, initial use is Provider to Provider data exchange
- Adopted into Meaningful Use of EHR Stage 2 data transport requirements
- NOTE: “Connect” was also created by ONC (will review on later call)

Rationale for Subgroup Dialog on DIRECT

- DIRECT is an example of an industry initiative that meets the following business and technical criteria for Phase IV Connectivity Rule:
  - Large scale adoption path - a transport based initiative included in national regulations (Meaningful Use Stage 2)
  - Clinical domain interoperability specification
  - Alignment with CORE use of digital certificates
ONC DIRECT: Project Overview

• Project Description
  – An ONC sponsored project with the intent of being able to push clinical data (e.g., CCDA) by secure email directly from sender to receiver
  • Initial focus is Provider to Provider clinical data exchange (e.g., in support of Transitions of Care).

• Project Mission
  – Focused on simple use cases where providers typically rely on fax to exchange information
  – Create a low barrier to entry for providers to implement; providers need to rely on EHR implementations.

• Timing
  – Meaningful Use Stage 2 will be rolling out throughout 2014/2015

• Specification Development Participation
  – Public and Private, Workgroups under ONC’s S&I; Example of Participating Entities (complete list available here): Allscripts, Emdeon, Epic, GE, CMS, Cerner, NIST, RelayHealth, Wellogic
ONC DIRECT: Planned Development Roadmap

Direct has four components as part of its roadmap:

1. Develop the specifications
   - Utilizes Simple Mail Transport Protocol (SMTP) to push payloads to recipients
   - S/MIME secures the message and the contents

2. Create a reference implementation (open source)

3. Industry Adoption
   - Meaningful Use 2 regulations required the use of Direct
   - 48 states have a sponsored Direct implementation either live, in pilot, or planned
     - Actual real-world use will also be tracked
   - Federal agencies (CMS, DoD, VA, IHS, SSA) have an interest or requirement to utilize Direct for exchange of PHI

4. Ongoing Policy Guidance
   - ONC has issued updated guidance in this area with Direct Implementation Guidelines to assure security and interoperability
   - Established HIE Governance Program to develop and adopt policies, interoperability requirements and business practices that align with national priorities, overcome interoperability challenges, reduce implementation costs and assure the privacy and security of health information
ONC DIRECT: Adoption Under Meaningful Use Stage 2

- Meaningful Use evolved from HITECH regulation with incentives for adoption of interoperability standards
  - Three stages are defined currently for Meaningful Use
    - Stage 1 is designed to capture structured information in EHRs
    - Stage 2 is designed to exchange structure information among providers and patients.
    - Stage 3 is to improve outcomes through analytics
- Stakeholders impacted by Meaningful Use Stage 2 requirements that specify the use of Direct
  - Certified EHR systems must enable Direct as part of Meaningful Use Stage 2 certification requirements
    - There are currently over 1,000 certified EHR systems for Stage 1; number of certified systems for Stage 2 is TBD
  - *Providers can use Direct or SOAP based transport options to meet MU2 requirements*
    - MU2 include sharing of transitions of care (TOC) documents
ONC DIRECT: Inclusion in MU Stage 2 Transport Requirements for Certified EHR Systems

Providers can use Direct or SOAP based transport options to meet MU2 requirements.

- Required
- Optional

### Meaningful Use Stage 2: (Transports)

- **Via eHealth Exchange Participant**
  - IHE XDR

- **SOAP**
  - SMTP
    - IHE XDM

- **Direct**
  - S/MIME

- **IHE XDR Profile** is an Integrated Healthcare Enterprise (IHE) specification named Cross Enterprise Document Reliable Interchange for the exchange of clinical documents using SOAP over HTTP (more information [here](#)).
- **IHE XDM Profile** is the Cross Enterprise Document Media Exchange specification created by IHE for the exchange of clinical documents using email and other media such as CD-ROM (more information [here](#)).
- **SMTP**: Simple Mail Transport Protocol
- **eHealth Exchange Participants** can be found [here](#).

© 2013 CORE. All rights reserved.
**ONC DIRECT: Messaging Infrastructure**

**Transport Protocol:** SMTP (Email)  
**Security:** Digital Certificates/Encryption/Signatures  
**Emerging Trust Framework:** DirectTrust

**Focus**
- Clinical Data Exchange
- Initial Use Case: Provider to Provider data exchange

**Direct Infrastructure includes Health Information Services Providers (HISP)**
- Internet based Service Providers with Secure Email capability, and with additional Direct messaging specific capabilities:
  - Addressing/routing (e.g., using Provider Directories, handling metadata translation between Email and SOAP based transport)
  - Security (e.g., Digital Certificate management, Digital Signatures)
- A Provider organization can be its own HISP or use an external HISP
  - HISP is not the same as CMS esMD Health Information Handler (HIH), which is authorized to share EMRs
- A HISP handles transport/security but does not process the transaction payload
ONC DIRECT: Key Features and Applicability

• Transaction applicability
  – Applicable for Batch processing mode for Clinical Data
    • Maximum size of Batch file will depend on SMTP implementations

• Security and Trust
  – Encryption and Signature using Digital Certificates
  – Establishing authentication and trust is critical
    • Trust can be established using Digital Certificates and Public Key Infrastructure (PKI)
      – Cost of various certification, entries, etc. unclear – or placing fees back into development process unclear
    • DirectTrust is emerging for Digital Certificates framework
      – Certifies Health Information Service Providers (HISP), Registration Authorities (RA) and Certificate Authorities (CA)
      – Publishes trusted CA certificates (known as “trust bundles”) used for establishing trust SSL connectivity
      – Partnered with Electronic Healthcare Network Accreditation Commission (EHNAC) to provide certifications
  – Use of HISP (Health Information Services Provider) message routing infrastructure is emerging for Direct transport
    • Providers must register a Direct email address

• Metadata
  – Clinical documents can be described using metadata (optional use of ‡IHE XDM)
    • Applicability of this metadata to administrative transaction payload is yet to be determined.

‡ IHE XDM is the Cross Enterprise Document Media Exchange specification created by IHE for the exchange of clinical documents using email and other media such as CD-ROM (more information here)
### Key Industry Connectivity Trends in Technical Areas

<table>
<thead>
<tr>
<th>Technical Focus Areas</th>
<th>Summary of Current Healthcare Industry State and Industry trends</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network And Transport</strong></td>
<td>*Internet. Most healthcare data exchange standards and profiles are HTTP based, but SMTP is emerging.</td>
</tr>
</tbody>
</table>
| **Transport Security**                      | • *SSL v3.0 is common  
• *TLS 1.0 for Government use  
• SMIME is emerging for SMTP |
| **Submitter Authentication/Authorization (Originating system, or Client)** | • *Username/Password is widespread  
• *X.509 Certificate over SSL gaining acceptance  
• Digital Signatures on documents are not common but emerging as requirements  
• Security Assertion Markup Language (SAML) is emerging for authorization information |
| **Standards for Envelope and Attaching files** | • *Increasing movement towards use of SOAP and MTOM as the envelope standard  
• *HTTP+MIME and SMTP+MIME based envelope are also in use |
| **Envelope Metadata**                        | • *Normative and payload agnostic metadata  
• Use case dependent – overlaps exist but still significant variations between different initiatives |
| **Message Interactions/Routing**             | * Common message interaction patterns include query/response and batch push / pull.  
For HTTP/SOAP based connectivity, WSDL is commonly used to specify the interactions. SMTP based transports are not well suited for real time/synchronous query/response, but can be used for “push” of Batch file. |

* Capability is already included in CAQH CORE Connectivity Rule 2.2.0
## Key Industry Connectivity Trends in Technical Areas (cont’d)

<table>
<thead>
<tr>
<th>Technical Focus Areas</th>
<th>Summary of Current Healthcare Industry State and Industry trends</th>
</tr>
</thead>
</table>
| **Message Envelope and Payload level Security** | • Envelope and Payload level security and digital signatures are gaining importance in the context of structured clinical document attachments.  
• As part of CAQH CORE Connectivity, the industry participants had considered Message Envelope level security requirements and had deferred it for future consideration.  
• The S&I esMD Author of Record initiative has developed draft white papers for identity proofing and digital signatures (for document attachments) using digital certificates, for electronic submission of documents to Medicare. These have not yet been vetted and widely accepted by the industry at this point. |
| **Schemas, Examples, Rule Text**            | *For SOAP based envelope specifications, the availability of specification standards like XSD and WSDL makes it possible to use them. Other (non-SOAP) approaches typically use examples* and descriptions in lieu of schemas.                                                                                                                                                                                                 |
| **Digital Certificates**                   | *Digital certificates are being used for transport level (SSL/TLS) security and are being considered for payload level (e.g., digital signatures) security. Initiatives like DirectTrust have developed policies for trust, but these have not yet been vetted and widely accepted by the industry.  
The esMD Author of Record has developed draft white papers for policy requirements for digital certificates in the context of identity proofing and digital signatures (for document attachments submitted to Medicare). |

* Capability is already included in CAQH CORE Connectivity Rule 2.2.0
Phase IV CAQH CORE Connectivity
Preliminary Opportunity Areas Based on Business & Market Analysis

• Improving Rule Language/Clarity
  – Improve clarity around Real-time and Batch requirements, error handling
  – Address CAQH CORE Connectivity Rule v2.2.0 implementer feedback

• Enhancing Envelope Standards and Metadata
  – *Expand ongoing payload agnostic approach for explicitly enumerating PayloadType transactions newly mandated by ACA
  – ‡Explore convergence of Envelope Standards

• Enhancing Reliability and Security
  – Reliable and secure handling of attachments
  – ‡Explore convergence of Authentication Standards
  – Explore policy for uniform use of digital certificates
  – Explore TLS as part of base requirement for transport security
  – Explore enhanced envelope level security (e.g., Signature, SAML Authorization), determining B2B nature of transactions and that some signatures may be applied at the document (payload) level.

• Exploring Additional Transport Options for Improved Alignment with Major National Initiatives
  – Explore support for additional transport options like ONC DIRECT

Note: This is only a preliminary list. Industry inputs are needed for identifying opportunities and evaluation and prioritization using CAQH CORE guiding principles, implementation complexity, cost saving potential etc. Additionally, any technical requirements need to be testable since CORE has a certification testing process.

‡ Convergence to a single envelope and authentication standard was the vision to improve interoperability that was set forth in previous CORE Connectivity phases, but was deferred to a future phase since industry wanted more experience in these standards.

* Possibly extracting out the PayloadType table into a separate document outside the Connectivity Rule.
Phase IV CAQH CORE Connectivity
Proposed Opportunity Areas for Rule Enhancement

Preliminary opportunities identified (highlighted)

- Public Internet (TCP/IP) – CORE Phase I Rule

- HTTP/S – CORE Phase I Rule
  (includes security of payload during transmission)
  - Explore support for additional transport options like ONC DIRECT
  - TLS part of baseline requirement

- Message Envelope & Message Metadata – CORE Phase II Rule
  (independent of payload – required by Phase I)
  - Explore convergence on single Envelope standard
  - Explore convergence on single authentication standard

- Message Envelope security - Digital Signatures and SAML
  (with consideration of envelope vs payload level security)

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

- Reliable handling of transactions (e.g., error handling)

- Security Policy for Trust and Uniform use of Digital Certificates

- Improve clarity of Real-time and Batch requirements

- Expand payload agnostic enumeration of transactions newly mandated by ACA

- Address implementer feedback
Appendix:
Additional Background on CAQH CORE Process and Federally Mandated CORE Connectivity Rule
## CAQH CORE Rules Approval Process

<table>
<thead>
<tr>
<th>*CAQH CORE Body</th>
<th>CAQH CORE Requirements for Rules Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1:</strong></td>
<td></td>
</tr>
<tr>
<td>Subgroups and Task</td>
<td>Not addressed in governing procedures, but must occur to ensure consensus building.</td>
</tr>
<tr>
<td>Groups</td>
<td></td>
</tr>
<tr>
<td><strong>Level 2:</strong></td>
<td>Work Groups require for a quorum that 60% of all organizational participants are voting. Simple majority vote (greater than 50%) by this quorum is needed to approve a rule.</td>
</tr>
<tr>
<td><strong>Level 3:</strong></td>
<td>Full CORE Voting Membership vote requires for a quorum that 60% of all Full CORE Voting Member organizations (i.e., CORE Participants that create, transmit, or use transactions) vote on the proposed rule at this stage. With a quorum, a 66.67% approval vote is needed to approve a rule.</td>
</tr>
<tr>
<td><strong>Level 4:</strong></td>
<td>The CAQH CORE Board’s normal voting procedures would apply. If the Board does not approve any proposed Operating Rule, the Board will issue a memorandum setting forth the reasons it did not approve the proposed Operating Rule and will ask the CORE Subgroups and Work Groups to revisit the proposed Operating Rule.</td>
</tr>
</tbody>
</table>

**NOTES:** Either the CAQH CORE Board or CAQH does not have veto or voting power over the CAQH CORE Operating Rules. Any entity that is a CAQH CORE participant per the CAQH CORE application process has a right to vote on the rules, understanding that at Level 3 only entities that will implement the rules vote on the rules. CORE Work Groups/Subgroups do not meet on a constant basis, only during rule writing or maintenance periods.
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Message Envelope Standards

• CAQH CORE Connectivity Rule v2.2.0 supports two envelope standards (subject to basic conformance requirements)
  – HTTP MIME Multipart and SOAP + WSDL are the two standards that met the majority of CAQH CORE technical criteria and had wide industry use
  – The SOAP envelope structure includes XSD schemas and the HTTP MIME envelope includes 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 Rule v2.2.0

Payload Processing Modes/Interactions

- CAQH CORE Connectivity Rule v2.2.0 addresses 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 156 Rule](#)  |
| 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)  
                  • Batch (asynchronous) processing is optional for X12 v5010 270/271 and X12 v5010 276/277 transactions  
                  • Batch (asynchronous) processing is required per CAQH CORE 350 Rule for X12 v5010 835 (ERA) |
Federally Mandated CAQH CORE Connectivity Rule v2.2.0

Message Structure

CAQH CORE Connectivity Rule v2.2.0 metadata is prescriptive to facilitate interoperability of administrative transactions

- Network
  - Communications (Transport) Protocol
  - Message Envelope + Message Metadata
  - Message Payload (Content)

- = Public Internet (TCP/IP) – CORE Connectivity Rules
- = HTTP over SSL (HTTP/S) – CORE Connectivity Rules) (includes security of payload during transmission)
- = Message Envelope & Message Metadata – CORE Connectivity Rule v2.2.0 Rule (independent of payload)
- = HIPAA Administrative Transactions (X12)
  - HL7 Clinical Messages
  - Zipped Files
  - Personal Health Record
  - Other Content
Federally Mandated CAQH CORE Connectivity Rule v2.2.0 Stakeholder Conformance Requirements

- CAQH CORE Connectivity Rule applies to health plans (HTTP/S server) and health care providers (HTTP/S client)
  - Rule defines 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)
Federally Mandated CAQH CORE Connectivity Rule v2.2.0

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

![Diagram showing server and client conformance requirements]

If your organization is a:

- Health Plan
- Clearinghouse/Switch

then you must implement **both** of these envelope standards

- HTTP Multipart MIME
- SOAP

If your organization is a:

- Healthcare Provider

then you must implement **one** of these envelope standards

- HTTP Multipart MIME
- SOAP
Federally Mandated CAQH CORE Connectivity Rule v2.2.0
Submitter Authentication

- CAQH CORE Connectivity Rule 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
Federally Mandated CAQH CORE Connectivity Rule v2.2.0

Error Handling

- Once request (e.g., X12 v5010 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 middle-ware or integration brokers)
  - 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 Processing Layer, it returns a response or error