“Front Line” Healthcare and Security Update

John Kelly, Harvard Pilgrim
James Rakshys, BCBSNC
Laurance Stuntz, CSC
Jeff Barnett, VeriSign (Symantec)
# Status of Today’s Presenters

<table>
<thead>
<tr>
<th>Organization</th>
<th>CORE PI Certified</th>
<th>CORE PII Certified</th>
<th>CORE PKI Management Pilot Participant</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCBSNC</td>
<td>✓</td>
<td>Committed</td>
<td>NA</td>
</tr>
<tr>
<td>CSC (NEHEN)</td>
<td>✓</td>
<td>Committed</td>
<td>✓</td>
</tr>
<tr>
<td>Harvard Pilgrim Health Care</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Symantec (VeriSign)</td>
<td>NA</td>
<td>NA</td>
<td>✓</td>
</tr>
</tbody>
</table>
CORE Guiding Principles Specific to Connectivity

- Developed using consensus-based approach among industry stakeholders and is designed to:
  - Facilitate interoperability.
  - Improve utilization of electronic transactions.
  - Enhance efficiency and help lower the cost of information exchange in healthcare.
  - Support not only Eligibility transactions, but also any other administrative transactions.

- Builds upon existing standards.
- Creates a base and not a “ceiling”:
  - E.g., 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 CORE rule for all new connections.
Phase II Connectivity Technical Principles

• General Principles:
  – Supports large Batch transaction files.
  – Supports Real-time transaction processing.
  – Supports large volume of single Real-time transaction processing.
  – Has extensive message attributes.
  – Supports Synchronous (i.e., request/response on a single connection) message exchanges.
  – Supports Asynchronous (i.e., response is initiated by responder on a separate connection) message exchanges.*
  – Supports Point-to-Point message exchanges.
  – Supports push and pull messaging.
  – Supports Rules based routing.*

• Security Principles:
  – Supports Submitter (Initiating System or Client) Authentication.
  – Supports Encrypted Authentication: credentials were encrypted at the transport layer using SSL.
  – Supports Digital Certificates.

• Implementation Business Principles:
  – Language Neutral.
  – Platform Neutral.

• Reliable Messaging:
  – Payload Independence.
  – Message Metadata.

• Interoperability Principles:
  – Compatible with emerging clinical standards for interoperability.

* In each phase, some advanced messaging features were deferred for consideration in future phases based on factors like market readiness, complexity.
Result: Costly management of multiple transport and envelope protocols; many of them proprietary. All-payer solutions very challenging. Costly parsing of data.
After CORE Phase II: Consensus on Transport, Envelope, Authentication Standards and Metadata

**Benefit:** Increased online and access that is less costly given uniformity in transport, envelope, authentication standards, and metadata. Reduced cost given reduction in time spent on implementations and data parsing.
# CORE Phase I and II Connectivity Summary

<table>
<thead>
<tr>
<th>Connectivity Rule Area</th>
<th>CORE Phase I Connectivity Rule</th>
<th>CORE Phase II Connectivity Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Internet</td>
<td>Internet</td>
</tr>
<tr>
<td>Transport</td>
<td>HTTP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Transport Security</td>
<td>SSL</td>
<td>SSL</td>
</tr>
<tr>
<td>Submitter (Originating System or Client) Authentication</td>
<td>Name/Password</td>
<td>Name/Password or 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) (e.g., PayloadType, Processing Mode, Sender ID, Receiver ID)</td>
</tr>
<tr>
<td>Message Interactions/ Routing</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td></td>
<td>Batch (Optional if used)</td>
<td>Batch (Optional if used)</td>
</tr>
<tr>
<td>Payload level Security</td>
<td>Unspecified</td>
<td>Considered and deferred</td>
</tr>
<tr>
<td>Acknowledgements, Errors</td>
<td>Specified</td>
<td>Enhanced Phase I, with 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>Maintained Phase I requirements</td>
</tr>
<tr>
<td>Companion Implementation Guide</td>
<td>Specified</td>
<td>Enhanced Phase I, with additional specificity</td>
</tr>
</tbody>
</table>

Acknowledgement requirements are at Connectivity and Payload Processing layers, and are defined in CORE Connectivity Rules as well as within other CORE Rules addressing acknowledgements.
Phase II Connectivity: Rationale for Two Envelope Standards

• Decision on supporting two message envelope standards:
  – SOAP+WSDL:
    • Well aligned with health-IT standards initiatives such as HL7, IHE, HITSP:
      ▪ Actively participated in all HITSP work groups.
      ▪ IHE interoperability demonstrations.
    • Well aligned with Federal direction, e.g., NHIN Exchange.
      ▪ SOAP + WSDL adopted for use.
  – HTTP MIME Multipart:
    • Relatively simple and well understood protocol framework.
    • CORE-certified entities have already implemented HTTP as part of Phase I.
  – Incremental “stepped” approach:
    • Facilitates adoption in a market that is still maturing.
    • Facilitates interoperability relative to the current state of envelope standard variability in the marketplace.
    • Rule establishes basic conformance requirements for these two envelope standards based on the role of each entity
CORE Phase II Connectivity Rule Specifies Envelope Metadata Syntax and Vocabulary

- CORE Phase II Connectivity Rule is consistent with SOAP 1.2; version will need to be updated over time.

- CORE Phase II metadata prescriptive to facilitate interoperability of administrative transactions, which is CORE’s focus.

  Network

  Communications (Transport) Protocol

  Message Envelope + Message Metadata

  Message Payload (Content)

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

= HTTP over SSL (HTTP/S) – CORE Phase I Rule (includes security of payload during transmission)

= Message Envelope & Message Metadata – CORE Phase II Rule (independent of payload – required by Phase I)

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

= Message Envelope (Envelope metadata is evolving) = HIPAA X12 Payload

simplifying healthcare administration

CAQH
### CORE Phase III Connectivity Rule: Proposed Technical Areas Considered by Subgroup

**Source of Proposed Features:** New national regulations/standards, industry trends, Inputs from NCPDP and others, Phase II Certification FAQs, Phase II deferred features

<table>
<thead>
<tr>
<th>Rule Area</th>
<th>High Priority (&quot;Must do&quot;)</th>
<th>Medium Priority (&quot;Could do&quot;)</th>
<th>Optional (&quot;May do&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Transport</td>
<td>N/A (same as Phase II).</td>
<td>N/A (same as CORE Phase II)</td>
<td>N/A (same as CORE Phase II)</td>
</tr>
<tr>
<td>Transport Security</td>
<td>Transport Layer Security (TLS) to be consistent with NHIN.</td>
<td>• Consistent Time (IHE ATNA)</td>
<td></td>
</tr>
<tr>
<td>Submitter (Originating system, or Client) Authentication/Authorization</td>
<td>• Convergence to a single authentication standard</td>
<td>• User level identity/authorization with SAML (OASIS)</td>
<td>• Privacy/Consent management</td>
</tr>
<tr>
<td></td>
<td>• Convergence to a single envelope standard</td>
<td>• Policy gaps in applying PKI/Certificates</td>
<td>• Lessons learned from industry PKI initiatives and security, such as HITRUST, and the VeriSign PKI Pilot</td>
</tr>
<tr>
<td>Envelope and Attachment Standards</td>
<td>• Convergence to a single envelope standard</td>
<td>• WS-Addressing</td>
<td>Addressing to support routing based on payload type</td>
</tr>
<tr>
<td>Envelope Metadata</td>
<td>• Include PayloadType for all 4010/5010 administrative transactions, whether HIPAA mandated or not; alternatively, the guidance for extending PayloadType values could be more specific. • Include new requirements and extensibility capability while remaining payload agnostic (e.g., NCPDP use cases). • For non-X12 adm transactions, refine algorithm for PayloadType.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Interactions/Routing</td>
<td>• Enhanced message exchanges identified by NCPDP, One-way push, Batch Mode transactions with Listing of Results files with ability to retrieve). • Support for Phase III Rules (e.g., 835).</td>
<td>• Routing through intermediaries (e.g., based on identifiers or payload type) • Asynchronous request/response using WS-Addressing • Common Data Transport Gap/Extension messaging interactions • Multi-hop and reliable messaging</td>
<td></td>
</tr>
<tr>
<td>Payload Security</td>
<td></td>
<td></td>
<td>• Payload level encryption</td>
</tr>
<tr>
<td>Schemas, Examples, Rule text</td>
<td>• MTOM for SOAP1.2 Real-time. • Review for Optional vs Required Fields. • CORE Phase II FAQ, Errata.</td>
<td>• Make SOAP+WSDL schemas extensible to facilitate user defined fields.</td>
<td></td>
</tr>
</tbody>
</table>
## Phase III Connectivity Focus: “Must Do”

<table>
<thead>
<tr>
<th>Area</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Envelope Metadata         | - Include payload type value types for all 4010 and 5010 administrative transactions, whether HIPAA mandated or not, or extend the PayloadType values within Phase II Connectivity and make more specific, particularly to support X12 administrative transactions.  
- Include new requirements and add extensibility capability while remaining payload agnostic (e.g., NCPDP use cases).  
- For non-X12 administrative transactions, refine algorithm for PayloadType from Phase II Connectivity and Security Rule. |
| New Message Interactions/Routing | Enhanced message exchanges identified by NCPDP, CMS esMD, e.g., one-way push, Batch mode transactions with listing of results files with ability to retrieve.  
Support for Phase III Rules (e.g., 835). |
| Schemas, Examples and Rule Text | MTOM for SOAP1.2 Real-time.  
CORE Phase II FAQ, errata. |
| Transport Security        | Require Transport Layer Security (TLS), to be consistent with Federal initiatives and industry direction.                                        |

Note: Subgroup is considering “base” CORE connectivity option for compatibility.
### Development Area

#### Critical External/Federal Developments

<table>
<thead>
<tr>
<th>Development Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Reform Bill (Section 1104)</td>
<td>• Administrative Simplification mandated, including concept of operating rules.</td>
</tr>
</tbody>
</table>
| American Recovery and Re-investment Act (ARRA), HITECH Rule | • HITECH Rule has increased emphasis on security and privacy and connectivity.  
• ONC Final Rule on Meaningful Use:  
  – Stage 1 does have stringent security requirements, but anticipated that Stage 2 and 3 will support HITECH emphasis. |
| Health Information Technology Standards Panel (HITSP) | • T85/SC114 Administrative Transport to Health Plan was based on CORE Phase II Connectivity Rule, with added security constraints.  
• Many aspects of HITSP are being used for HITECH requirements.  
• Common Data Transport Gap/Extension - Technical Note (TN907). |

**NOTE:** HITSP’s contract with HHS concluded on April 30, 2010. Much of HITSP’s work is being integrated into other ONC efforts.
## Key External Developments During 2009-2010

*(continued)*

<table>
<thead>
<tr>
<th>Development Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical External/Federal Developments</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **CORE-National Council for Prescription Drug Programs (NCPDP) joint work** | • HITSP T85 (based on CORE Phase II connectivity rule) extended for Provider/Pharmacy transactions with health plans.  
• Application of T85 to pharmacy transactions has identified some gaps, which are being addressed in Phase III via NCPDP and CORE coordination. |
| **Federal Health Architecture (FHA)** | • Architecture, security and connectivity for government agencies.  
• Nationwide Health Information Network (NHIN) moving forward:  
  – NHIN CONNECT: Open source gateway.  
  – Working in collaboration with CMS MITA (see below). |
| **NHIN Exchange** | • Moving forward with emphasis on HITECH needs; focused on having provider-to-provider communications (use cases such as referrals); SMTP being evaluated. |
| **CMS Medicaid Information Technology Architecture (MITA)** | • MITA has incorporated FHA NHIN CONNECT with extensions to support administrative transactions:  
  – CORE Phase II Connectivity Rule (with extensions) incorporated; HIMSS Showcase demonstrated this. |
### Key Developments During 2009-2010 (continued)

<table>
<thead>
<tr>
<th>Development Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical External/Federal Developments</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **CMS es-MD Pilot Project**                                 | - Electronic Claims Attachment submission (EHR) from providers to CMS:  
  - Common connectivity required to align with HITECH; CMS driving move to electronic transactions and support of standards.  
  - CORE working to coordinate with pilot needs. |
| **CORE – Specific**                                         |                                                                                                                                                                                                             |
| **CORE Phase II Implementations, Certifications**           | - Many entities have implemented CORE Phase II Connectivity Rule and have been certified. Common questions raised have been addressed in FAQs.                                                             |
| **Maintenance Updates to CORE Phase II Rule (Version 2.0.1)** | - Feedback from early adopters and CORE certification participants, FAQs. Batch schemas and metadata were updated. 5010 support updated.                                                                          |
| **CORE PKI Security and Authentication Pilot**              | - Pilot to identify administrative simplification policies for digital certificates.                                                                                                                         |
Why a CORE PKI Pilot and Who Are The Sponsors?

• In the next few years, it is estimated that more than 700,000 physicians and more than 185 million consumers will go online to exchange sensitive health information:
  – How will the industry ensure: Security, interoperability, privacy and authentication of organizations and users?

• Currently, there is no industry consensus on requirements for the industry to authenticate administrative data exchange:
  – CORE has an established process for creating and driving adoption of common connectivity/security methods that are aligned with clinical efforts, e.g., ONC’s NHIN (requires single CA and Entrust is accepted).
  – CORE is sponsored by CAQH, which also sponsors UPD:
    • UPD has a critical mass of providers who want simplified connectivity/security.
    • MA: Approximately 28,500 MDs/DOs operate in state and 85% use UPD.
  – NEHEN is a leader in data exchange and related policy setting, and many of its participants are CORE-certified.
  – VeriSign/Symantec is a leader in PKI/authentication services.
What Are The Objectives?

• **Background:**
  - System-to-System authentication using digital certificates is required by CORE Phase II Connectivity Rules; future phases will consider user-level authentication.
  - Effective enforcement of authentication requires “rules of the road” for trust and certificate practices. Administrative simplification will be needed for authentication given the number of users and the levels of trust involved.

• **Objectives:**
  - Identification of policy and standard gaps in the implementation of X.509 Digital Certificates for a vendor neutral PKI environment for streamlined node authentication:
    • Evaluate policy and standards requirements for interoperability, while supporting a limited set of PKI providers (Certificate Authorities) to ensure vendor neutrality.
    • Validate solution by piloting within NEHEN using Symantec PKI, but with ability to add other PKI vendors at the topmost level of PKI hierarchy (i.e., as Root CAs).
    • Evaluate requirements for a single digital credential per healthcare provider issued by one of a few PKI vendors, such that Health Plans recognize and accept that credential.
    • Evaluate feasibility of leveraging datasources such as CAQH’s UPD for identity proofing of providers and assisting with certificate management.
  - Ongoing alignment with and input towards direction of national regulations and standards. Lessons learned will be incorporated into future NEHEN policy debates, CORE Connectivity requirements and publically shared.
Pilot: Timeline, Key Steps and Resources Required

• Time:
  – Six months.

• Key steps:
  – Agreement on pilot participants and milestones.
  – Data gathering, e.g., interviews, questionnaire on-site at each participant location.
  – Use case agreement, e.g., mix of sensitive/non-sensitive administrative data.
  – Written summary of results and identification of potential policy implications.

• Primary time and resources required: leadership, technical, and external communications:
  – Technical: Expert hours per participant for interviews/discovery, based upon CORE PKI Assessment Participant Questionnaire, and engineering configuration to work with certificates.
  – CAQH CORE is providing VeriSign/Symantec resources, NEHEN is managing pilot participants and all three organizations will collaborate on project management.
  – Review and input on summary of findings.
Pilot Success Factors

• Generate a focus on the need for national, cost-effective and adaptable PKI policies solutions that build trust.

• Demonstrate that:
  – Certificate enrollment and management process for Healthcare Providers (clients) and Health Plans (servers) can be streamlined.
  – Healthcare Providers (clients) can use a single digital identity to access multiple Health Plans (servers), where the digital identity is obtained from a limited set of Certificate Authorities (i.e., vendor neutral).
  – Health Plans (servers) have reduced administrative overheads to allow connections from Healthcare Providers (clients), using credentials from a limited set of Certificate Authority vendors.

• Identify any gaps in policy/implementation to inform future national debate and CORE rule development.
E-Authentication Assurance Levels

- Low
  - PIN/User ID
  - Access to Protected Website

- Medium
  - One-Time Password
  - Applying for a Loan Online

- High
  - Knowledge-Based
  - Obtaining Govt. Benefits

- Very High
  - Multi-Factor Token
  - PKI/ Digital Signature
  - Biometrics
  - HSPD-12 PIV Card

Increased Need for Identity Assurance