

simplifying healthcare administration

CAQH[®]

Massachusetts Health Data Consortium
CAQH CORE - NEHEN - VeriSign/Symantec Pilot

September 2010

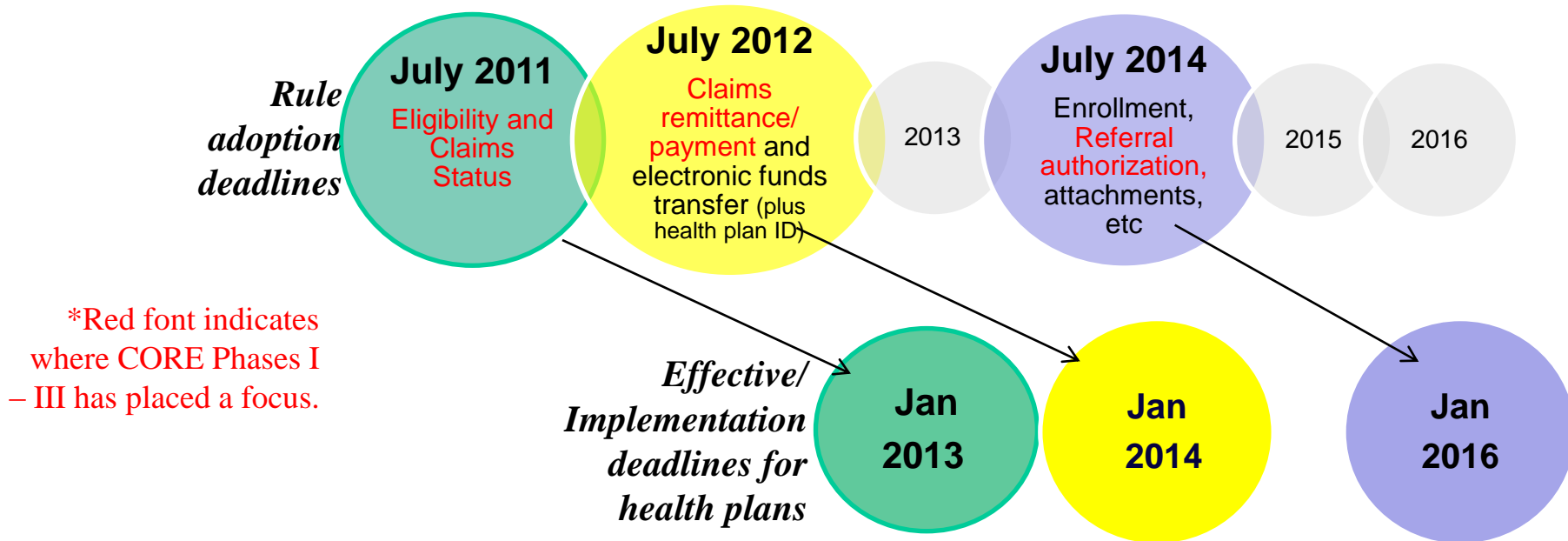
Agenda

- CAQH status
 - CORE
 - UPD
- Pilot overview
- Q&A

HR 3590 Patient Protection and Affordable Care Act: Section 1104

The concept of operating rules is addressed in the health reform bill in section 1104, which focuses on administrative simplification. Requires the Secretary to adopt and regularly update standards, implementation specifications, and operating rules for the electronic exchange and use of health information for the purposes of financial and administrative transactions.

Rule writing and mandated implementation occur



*Red font indicates where CORE Phases I – III has placed a focus.

simplifying healthcare administration

CAQH

Why a Pilot and Why These 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 HITSP and NHIN
 - 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/Symatec is a leader in PKI/authentication services

What is the Pilot? 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 is needed 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 (ie 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 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.

What Are the Benefits to Pilot Participants?

- “Front seat” in developing a trust framework needed by the industry.
- Voice in how operating rules and related initiatives are implemented, using real-world feedback.
- Understand your organizations’ implementation requirements and pain points.
- Ensure barrier to adoption such as cost and administrative simplification are considered as these new technologies roll-out.

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
 - 30+ hrs technical: 10-20 man-hours per participant for interviews/discovery, based upon CORE PKI Assessment Participant Questionnaire; 10 hours per application, for engineering and 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

E-Authentication Assurance Levels

